CONFIRMA

POLÍTICA DE CERTIFICACIÓN CERTIFICADO CUALIFICADO TRIBUTARIO

CONTROL DOCUMENTAL

NOMBRE DEL ARCHIVO:	
POLÍTICA DE CERTIFICACIÓN DE CERTIFICADO CUALIFICADO TRIBUTARIO DE CONFIRMA S.A.	
CÓDIGO: DOC-PCT -CF	**VERSIÓN: 1.0**
UBICACIÓN FISICA: CONFIRMA S.A.	**FECHA: 14/04/2023**
CLASIFICACION DE SEGURIDAD: Público	

CONTROL DE VERSIONES			
FECHA	**VERSION**	**RESPONSABLES**	**MOTIVO DE CAMBIO**
14/04/2023	1.0	CONFIRMA S.A.	Primera Edición del Documento

DISTRIBUCIÓN DEL DOCUMENTO	
ÁREA	**NOMBRES**
Personal con Rol de Confianza establecidos en la DPC del PCSC CONFIRMA S.A.	PCSC de CONFIRMA S.A.
Documento Público	https://www.confirma.com.py/

PREPARADO POR:	**REVISADO POR:**	**APROBADO POR:**
UANATACA S.A.	CONFIRMA S.A.	CONFIRMA S.A.

INDICE

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que obligatoriamente deberán ser observados por los Prestadores Cualificados de Servicios de Confianza (PCSC) en su carácter de Autoridad de Certificación Intermedia (ACI) y como integrantes de la Infraestructura de Clave Pública del Paraguay (ICPP) para la formulación y la elaboración de su política de certificación (PC)

Toda Política de Certificación elaborada en al ámbito de la Infraestructura de Clave Pública del Paraguay (ICPP) debe obligatoriamente adoptar la misma estructura empleada en el documento.

Esta PC es aplicable a los siguientes certificados:

- Certificados Cualificados Tributarios:
    - F1

Los tipos de certificados "F" o "S" definen escalas de seguridad (1, 2 y 3), asociados con requisitos menos o más estrictos atendiendo al tipo de certificado. El nivel de seguridad estará caracterizado por los requisitos mínimos definidos para aspectos como:algoritmo y tamaño de la clave criptográfica, medios de almacenamiento de clave, proceso de generación del par de claves, procedimiento de identificación del titular del certificado, frecuencia de emisión de la lista de certificados revocados (LCR) y el plazo de validez del certificado.

El par de claves criptográficas relacionadas a los tipos de certificado F1 o S1 deberá obligatoriamente ser almacenado en un:

- dispositivo Smart Card sin capacidad de generación de claves y protegidos por contraseña y/o identificación biométrica; o
- token sin capacidad de generación de claves y protegidos por contraseña y/o identificación biométrica; o
- un repositorio protegido por contraseña y/o identificación biométrica cifrado por software.

Las claves privadas relacionadas a los certificados del tipo F1, F2, S1, S2 no podrán ser generadas ni gestionadas por los PCSC por lo que serán de exclusiva responsabilidad del titular del certificado o del responsable del mismo.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre del Documento	POLÍTICA DE CERTIFICACIÓN DE CERTIFICADO CUALIFICADO TRIBUTARIO DE CONFIRMA S.A.
Versión del Documento	V1.0
Fecha de Aprobación	14/04/2023
OID (Object Identifier):	1.3.6.1.4.1.58404.1.1.2.1
Ubicación de la DPC relacionada	https://www.confirma.com.py/wp-content/uploads/2023/01/Declaracion_de_practicas_de_certificacion_Confirma_SA.pdf

1.3. PARTICIPANTES DE LA PKI

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

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

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

Un PCSC presta servicios de CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS CUALIFICADAS y/o SELLO ELECTRÓNICO CUALIFICADO y CERTIFICADOS RELATIVOS A ESTOS SERVICIOS.

1.3.2. AUTORIDADES DE REGISTRO (AR)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la validación y verificación de la identidad de los solicitantes de certificados digitales y si procede, de los atributos asociados a los mismos. Las Autoridades de Registro (RA) llevan a cabo procesos de recepción, identificación y remisión de solicitudes de emisión o revocación de certificados electrónicos y de identificación de sus solicitantes.

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

Los datos referentes a las AR habilitadas por el PCSC se encuentran en la dirección de página web (URL):
https://www.confirma.com.py/autoridades-de-registro/
El PCSC de CONFIRMA S.A. mantiene publicada en el sitio principal de internet las siguientes informaciones actualizadas.

a) la lista de todas las ARs habilitadas;

b) Lista de las ARs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

La AV puede ser una entidad propia o externa al PCSC de CONFIRMA S.A. responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por el PCSC.

Las informaciones actualizadas sobre:

- Lista de todas las Avs Habilitadas
- Lista de las AVs que se han inhabilitado por el PCSC de Confirma S.A. indicando su fecha de inhabilitación.

La URL es la siguiente:
https://www.confirma.com.py/autoridades-de-validacion/

1.3.4. TITULARES DEL CERTIFICADO

Son personas físicas o jurídicas las que podrán ser titulares de los certificados emitidos por el PCSC de CONFIRMA S.A. según corresponda a un certificado cualificado de firma electrónica o de sello electrónico cualificado respectivamente conforme a esta PC.

1.3.5. PARTE USUARIA

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

1.3.6. OTROS PARTICIPANTES

1.3.6.1. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

Las PSS son entidades externas a las que recurre la AC o la AR de CONFIRMA S.A. para desempeñar actividades descritas en esta PC o en una DPC y se clasifican en tres categorías, conforme al tipo de actividades prestadas.

a) disponibilización de infraestructura física y lógica;

b) disponibilización de recursos humanos especializados; y

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

Las informaciones actualizadas de las PSS a la que recurre el PCSC de CONFIRMA S.A. se encuentran en la dirección de página web (URL): https://www.confirma.com.py/prestadores-de-servicios-de-soporte/

El funcionamiento de un PSS vinculado al PCSC de CONFIRMA S.A. se realiza mediante un acuerdo operacional, el cual es autorizado por la AC Raíz-Py con la habilitación correspondiente.

El PCSC de CONFIRMA S.A. tambien publica en su sitio web información referente a:

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

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

Las Políticas de Certificación del PCSC CONFIRMA S.A. correspondientes a cada tipo de certificado que emita son las que determinan los usos apropiados que debe darse a cada certificado.

Las aplicaciones y otros programas que soporten el uso de un certificado electrónico de cierto tipo contemplado por la ICPP deben aceptar cualquier certificado del mismo tipo, o superior, emitido por cualquier PCSC habilitado por la AC Raíz-Py.

En la definición de aplicaciones para el tipo de certificado definido por la PC, el PCSC CONFIRMA S.A. responsable debe tener en cuenta el nivel de seguridad previsto para ese tipo de certificado conforme a lo estipulado en el ítem 1.1. Certificados Tributarios de los tipos F1 serán utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de integridad de sus informaciones.

Certificados del tipo S1 serán utilizados en aplicaciones como confirmación de identidad y sello de documentos electrónicos con verificación de integridad y origen de sus informaciones.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos por el PCSC de CONFIRMA S.A. deben ser utilizados dentro del marco de la normativa vigente que rige la materia. Cualquier otro uso de los certificados no especificado en esta PC y en la normativa vigente, está fuera del alcance y responsabilidad de esta PC.

1.5. ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PSC: CONFIRMA S.A.

1.5.2. PERSONA DE CONTACTO

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: https://www.confirma.com.py/

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

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

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: https://www.confirma.com.py/

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA PC

Los procedimientos para la aprobación de PC del PCSC DE CONFIRMA S.A. son establecidos a criterio de AC Raíz-Py de la ICPP.

1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1. DEFINICIONES

- **Agente de registro:** persona responsable de la realización de las actividades inherentes a la AR. Realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.
- **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
- **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
- **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.
- **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la

cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.

- **Autoridad de Certificación Intermedia**: entidad cuyo certificado ha sido emitido por la AC Raíz-Py, es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador cualificado de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.
- **Autoridad de Registro:** entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.
- **Autoridad de Validación:** entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por la AC. La AV puede ser propia del PCSC o delegada a un tercero.
- **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
- **Cadena de certificación:** lista ordenada de certificados que contiene un certificado del firmante o creador de sello y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante o creador de sello es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El firmante, creador de sello o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.

- **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley No 6822/2021.
- **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley No 6822/2021.
- **Certificado cualificado tributario:** certificado expedido por un Prestador Cualificado de Servicios de Confianza, el cual podrá ser utilizado para todos los fines convencionales ante el Sistema Marangatu, Sistema Integrado de Facturación Electrónica Nacional, otros Sistemas de Información administrados por la Subsecretaría de Estado de Tributación (SET) así como otros usos afines autorizados por la Autoridad de Aplicación.
- **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.
- **Contrato de prestación de servicio de confianza:** Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado que contiene información relativa al solicitante del certificado y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.
- **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
- **Clave pública y privada:** la criptografía en la que se basa la ICPP, es la criptografía asimétrica. En ella, se emplean un par de claves:

lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.

- **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
- **Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.
- **Declaración de Prácticas de Certificación:** 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.
- **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión, suspensión o revocación del certificado cualificado electrónico será considerada la cédula de identidad civil o el pasaporte del solicitante.
- **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
- **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
- **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma

electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

- **Firmante:** una persona física que crea una firma electrónica.
- **Generador:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la AC, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.
- **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
- **Identificador de Objeto:** sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.
- **Identificación del Titular de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a través de la presencia física del interesado o mediante otros medios que aporten una seguridad equivalente en términos

de fiabilidad a la presencia física, conforme a los supuestos establecidos en la Ley y en base a los documentos de identificación previstos en la presente DPC.

- **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.
- **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
- **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
- **Lista de Confianza**: Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley No 6822/21.
- **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
- **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
- **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.

- **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley No 6822/2021.
- **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley No 6822/2021.
- **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
- **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
- **Política de Certificación:** documento en el cual la AC define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
- **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
- **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
- **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o

la AR y autorizada por la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.

- **Registro de Auditoría:** registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.
- **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
- **Rol de confianza:** función crítica que desempeña personal de la AC, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la AC.
- **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
- **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una AC.
- **Solicitud de Firma de Certificado:** petición de certificado electrónico que se envía a la AC, mediante la información contenida en el CSR, la AC, puede emitir el certificado electrónico una vez realizadas las comprobaciones que correspondan.
- **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte de documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados de sello electrónico para persona jurídica.

- **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
- **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su creación.
- **X.500:** estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525.
- **X.509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2.SIGLAS Y ACRÓNIMOS

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AGR	Agente de Registro
P	País (C por su sigla en inglés, Country)
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
ACI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad civil

NC	Nombre Común (CN por sus siglas en inglés, Common Name)
PC	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, Certification Practice Statement)
LCR	Lista de certificados revocados (CRL por sus siglas en inglés, Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PAS	Pasaporte
ICPP	Infraestructura de Clave Pública del Paraguay
PCSC	Prestador cualificado de servicios de confianza
PSS	Prestador de Servicios de Soporte

Py	ParAguay
AR	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RA	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RUC	Registro único del contribuyente
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator)
AV	Autoridad de validación (AV por sus siglas en inglés, Validation Authority)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC CONFIRMA S.A. o son detallados los aspectos específicos para la PC, si los hubiere.

2.1. REPOSITORIOS

Como establezca la DPC del PCSC CONFIRMA S.A.

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

2.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

Como establezca la DPC del PCSC CONFIRMA S.A.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A. o son detallados los aspectos específicos para la PC, si los hubiere.

3.1 NOMBRES

3.1.1.TIPOS DE NOMBRES

Como establezca la DPC del PCSC CONFIRMA S.A.

3.1.1. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Como establezca la DPC del PCSC CONFIRMA S.A.

3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Como establezca la DPC del PCSC CONFIRMA S.A.

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Como establezca la DPC del PCSC CONFIRMA S.A.

3.1.5 UNICIDAD DE NOMBRES

Como establezca la DPC del PCSC CONFIRMA S.A.

3.1.6 PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

Como establezca la DPC del PCSC CONFIRMA S.A.

3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS

Como establezca la DPC del PCSC CONFIRMA S.A.

3.2.8. PROCEDIMIENTOS ESPECIFICOS

Como establezca la DPC del PCSC CONFIRMA S.A.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

Como establezca la DPC del PCSC CONFIRMA S.A.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Como establezca la DPC del PCSC de CONFIRMA S.A.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A. o son detallados los aspectos específicos para la CP, si los hubiere.

4.1 SOLICITUD DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Como establezca la DPC del PCSC CONFIRMA S.A.

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.3 EMISIÓN DEL CERTIFICADO

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

Como establezca la DPC del PCSC CONFIRMA S.A.

4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISION DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6 RENOVACIÓN DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6.4 NOTIFICACIÓN AL TITULAR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Este ítem no aplica

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

Este ítem no aplica

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

Este ítem no aplica

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

Este ítem no aplica

4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO

Este ítem no aplica

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE- EMITIDO

Este ítem no aplica

4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS

Este ítem no aplica

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

Este ítem no aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

Este ítem no aplica

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica

4.8.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO

Este ítem no aplica

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Este ítem no aplica

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

Este ítem no aplica

4.8.7 NOTIFICACIÓN POR EL PCSC DE UNA EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

Este ítem no aplica

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.8 LATENCIA MÁXIMA PARA LCR

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

No aplica.

4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

4.10 SERVICIOS DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

Como establezca la DPC del PCSC CONFIRMA S.A.

4.10.2 DISPONIBILIDAD DEL SERVICIO

Como establezca la DPC del PCSC CONFIRMA S.A.

4.10.3 CARACTERÍSTICAS OPCIONALES

Como establezca la DPC del PCSC CONFIRMA S.A.

4.11 FIN DE ACTIVIDADES

Como establezca la DPC de CONFIRMA S.A.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Este ítem no aplica

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

En los apartados siguientes son referidos a los ítems correspondientes de la DPC del PCSC responsable o ser detallados los aspectos específicos para la PC, si los hubiere

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.2 ACCESO FÍSICO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.2.1 NIVELES DE ACCESO FÍSICO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.2.2 SISTEMAS FÍSICOS DE DETECCIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.2.3 SISTEMAS DE CONTROL DE ACCESO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.2.4 MECANISMOS DE EMERGENCIA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.4 EXPOSICIÓN AL AGUA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.6 ALMACENAMIENTO DE MEDIOS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.7 ELIMINACIÓN DE RESIDUOS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.1.8 RESPALDO FUERA DE SITIO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Como establezca la DPC del PCSC CONFIRMA S.A.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3. CONTROLES DE PERSONAL

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Como establezca la DPC del PCSC CONFIRMA S.A.

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Como establezca la DPC del PCSC CONFIRMA S.A.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.4.8. EVALUACIÓN DE VULNERABILIDADES

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5. ARCHIVOS DE REGISTROS

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5.2. PERIODOS DE RETENCIÓN PARA ARCHIVOS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5.3 PROTECCIÓN DE ARCHIVOS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Como establezca la DPC del PCSC CONFIRMA S.A.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.6 CAMBIO DE CLAVE

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

Como establezca la DPC del PCSC CONFIRMA S.A.

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Como establezca la DPC del PCSC CONFIRMA S.A.

5.8. EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

Como establezca la DPC del PCSC CONFIRMA S.A.

6. CONTROLES TÉCNICOS DE SEGURIDAD

En los siguientes ítems, la PC define las medidas de seguridad necesarias para proteger las claves criptográficas de los titulares de certificados emitidos según la CP. También son definidos otros controles técnicos de seguridad utilizados por el PCSC de CONFIRMA S.A.y por las ARs a ella vinculadas para la ejecución de sus funciones operativas.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

Cuando el titular del certificado sea:

- persona física, esté será el responsable de generar el par de claves criptográficas, salvo en caso de su gestión en nombre del firmante, en donde las claves privadas asociadas a los certificados son generadas y custodiadas por el módulo de activación de firma del PCSC, de forma que el acceso a dichas claves se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante.

El algoritmo para utilizar las claves criptográficas de titulares de certificados, está definido conforme al documentoDOC-ICPP-06(1)

Cuando es generada, la clave privada del titular del certificado de la deberá ser grabada cifrada mediante un algoritmo simétrico conforme al documento DOC-ICPP-06 [1], en un medio de almacenamiento definido para cada tipo de certificado previsto en la ICPP conforme a lo estipulado en la Tabla N° 2 de este ítem.

La clave privada deberá viajar cifrada, utilizando los mismos algoritmos mencionados en el párrafo anterior, entre el dispositivo generador y el medio utilizado para su almacenamiento.

Los medios de almacenamiento de claves privadas cumplirán los siguientes requisitos garantizando como mínimo, por medios técnicos y de procedimiento adecuados, que:

a) la confidencialidad de las claves privadas utilizadas para la creación de firmas electrónicas o sellos electrónicos, esté garantizada razonablemente .

b) las claves privadas utilizadas para la creación de firma electrónica o sello electrónico sólo puedan aparecer una vez en la práctica.

c) exista la seguridad razonable de que claves privadas utilizadas para la creación de firma electrónica o sello electrónico no pueden ser hallados por deducción y de que la firma o sello está protegido con seguridad contra la falsificación mediante las tecnologías disponibles en el momento.

d) las claves privadas utilizadas para la creación de firma electrónica o sello electrónico puedan ser protegidas por el firmante legítimo de forma fiable frente a su utilización por otros.

Estos medios de almacenamiento de claves privadas no alterarán los datos que deben firmarse o sellarse ni impedirán que dichos datos se muestre al firmante o creador de sello antes de firmar o sellar.

La generación o la gestión de las claves privadas de firma electrónica o sello electrónico en nombre del firmante sólo podrán correr a cargo del

PCSC de CONFIRMA S.A. , en los términos establecidos en el documento DOC-ICPP-07 [2].

Tabla N° 2 – Medio de almacenamiento de claves criptográficas.

TIPO DE CERTIFICADO	MEDIO DE ALMACENAMIENTO
F1	○ Tarjeta inteligente o token, ambos sin capacidad de generación de claves y protegidos por contraseña y/o identificación biométrica; o ○ repositorio protegido por contraseña y/o identificación biométrica, encriptado por software en la forma definida anteriormente.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ítem no aplicable, no existe la generacion ni entrega alguna de la clave privada al titular o responsable del certificado.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La entrega de la clave pública del titular del certificado al PCSC de CONFIRMA S.A. En los casos en los que se genere una solicitud de

certificado (CSR) por el titular, deberá adoptarse el formato definido en el documento DOC – ICPP – 06 [1]

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

La clave pública del PCSC de CONFIRMA S.A. está a disposición de la parte usuaria (ver apartado 2.1)

Las formas para la entrega de un certificado emitido por el PCSC de CONFIRMA S.A. podrá comprender, entre otras:

a) en el momento de disponibilización de un certificado a su titular, usando el formato definido en el documento DOC-ICPP-06 [1];

b) un directorio;

c) una página WEB del PCSC; y

d) otros medios seguros aprobados por la AC Raiz – Py.

6.1.5. TAMAÑO DE LA CLAVE

Los algoritmos y tamaños de clave a ser utilizados por el PCSC de CONFIRMA S.A. en los diferentes tipos de certificados emitidos en el marco de la ICPP , se definen en el documento DOC-ICPP-06.

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

Los parámetros de generación y verificación de calidad de claves asimétricas de las personas físicas o jurídicas titulares de certificados, adoptarán el estándar definido en el documento DOC-ICPP-06.

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

Los usos admitidos de la clave para los certificados cualificados tributarios F1 vienen dados por el valor de las extensions Key Usage y Extended Key Usage de los mismos. El contenido de dichas extensiones para los de firma electrónica F1 se puede consultar en el apartado 7.1 del presente documento.

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

En los apartados siguientes, la PC del PCSC debe define los requisitos para la protección de las claves privadas de los titulares de certificados emitidos según su PC.

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

El estándar requerido para los módulos criptográficos con certificados cualificados tributarios F1, es el FIPS 140-1 o FIPS 140-2, de acuerdo al document DOC-ICPP-06[1]. Los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada del titular o responsable del certificado, observando los estándares definidos en el documento DOC-ICPP-06 [1].

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

Ítem no aplicable.

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

El PCSC CONFIRMA S.A. no almacena ni copia las claves privadas de los titulares de certificados de firma digital (tipo F1).

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

Cualquier titular de un certificado, a su criterio, puede mantener una copia de su propia clave privada.

El PCSC de CONFIRMA S.A. no puede conservar una copia de seguridad de la claves privadas asosciadas a los certifciados de tipo F1..

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

El PCSC no almacena las claves privadas asociadas a certificados de los tipos F1.
Defínase archivado como el almacenamiento de la clave privada para su uso futuro, después del periodo de validez del certificado correspondiente.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Conforme al ítem 6.1

6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de al menos un factor de seguridad pudiendo ser contraseñas, tokens, biometría, etc.).

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Este ítem no aplica.

6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

Cada titular del certificado debe definir los procedimientos necesarios para la destrucción de su clave privada.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas de los titulares de los certificados cualificados tributarios F1, así como las LCRs emitidas, serán almacenadas y gestionadas por el PCSC CONFIRMA SA, luego de la expiración de los certificados correspondientes por un periodo de 10 (diez) años desde su última emisión, para la verificación de firmas generados durante su periodo de validez.

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

Las claves privadas de sus titulares deberán ser utilizadas únicamente durante el periodo de validez correspondiente. Las correspondientes

claves públicas podrán ser utilizadas durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

Tabla N°3 – Período de validez de los certificados

Tipo de certificado	Tiempo de uso en años	Tiempo operacional en años	Periodo máximo de validez del certificado (en años)
F1	1	1	Emitido por un tiempo máximo de 1 (un) año, al finalizar ese período pierde su validez.

6.4 DATOS DE ACTIVACIÓN

En los siguientes ítems de la PC de PCSC de CONFRIMA S.A , son descritos los requerimientos de seguridad referentes a los datos de activación. Los datos de activación, distintos a las claves criptográficas, son aquellos requeridos para la operación de algunos módulos criptográficos.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para certificados cualificados tributarios F1 la generacion y almacenamiento del par de claves son realizados en software, con capacidad de generacion de claves, siendo activados y protegidos por contraseñas y/o identificación biométrica.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la clave privada del titular del certificado están protegidos contra el uso no autorizado, por medio de mecanismos de criptografía y de control de acceso físico.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulaciones

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La PC del PCSC de CONFIRMA S.A. describe los requisitos de seguridad computacional del equipamiento donde será generado el par de claves criptográficas de los titulares de certificados, observando los requerimientos generales previstos en la DPC.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Como establezca la DPC del PCSC CONFIRMA S.A.

6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Como establezca la DPC del PCSC CONFIRMA S.A.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

Como establezca la DPC del PCSC CONFIRMA S.A.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Como establezca la DPC del PCSC CONFIRMA S.A.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Como establezca la DPC del PCSC CONFIRMA S.A.

6.6.4. CONTROLES EN LA GENERACIÓN DE LCR

Como establezca la DPC del PCSC CONFIRMA S.A.

6.7 CONTROLES DE SEGURIDAD DE RED

En el caso que el ambiente de utilización del certificado definido por la PC exija controles específicos de seguridad de red, estos controles deben de ser descritos en este ítem de la PC, de acuerdo con las normas, criterios, prácticas y procedimientos de la ICPP.

6.7.1. DIRECTRICES GENERALES

Como establezca la DPC del PCSC CONFIRMA S.A.

6.7.2. FIREWALL

Como establezca la DPC del PCSC CONFIRMA S.A.

6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

Como establezca la DPC del PCSC CONFIRMA S.A.

6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Como establezca la DPC del PCSC CONFIRMA S.A.

6.8. FUENTES DE TIEMPO

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

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

En los siguientes ítems deben son descritos los formatos de los certificados y de las LCR/OCSP generados según el PC.

Son incluidas las informaciones sobre las normas adoptadas, sus perfiles, versiones y extensiones. Los requisitos mínimos establecidos en los siguientes ítems son obligatoriamente considerados en todos los tipos de certificados admitidos en el ámbito de la ICPP.

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PCSC de CONFIRMA S.A. , según sus respectivas PCs, estan conformes al formato definido por la norma ITU X.509 o ISO/IEC 9594-8, según el perfil establecido en RFC 5280.

A continuación, se detalla el contenido de las extensiones más significativas de los certificados cualificados Tributarios F1 emitidos por la PCSC CONFIRMA S.A. Certificado Cualificado Tributario F1 La estructura del certificado, referente a la extensión sujeto del certificado, es la que se describe como ejemplo en la siguiente tabla:

SUJETO del Certificado Cualificado Tributario F1		
Campo	**Valor de Ejemplo**	**Descripción**
Country (C) {OID: 2.5.4.6}	PY	Código de País es asignado de acuerdo al estándar ISO 3166
Organization (O) {OID: 2.5.4.10}	CERTIFICADO CUALIFICADO TRIBUTARIO	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un CERTIFICADO CUALIFICADO TRIBUTARIO, en mayúscula y sin tilde.
Organization Unit (OU) {OID: 2.5.4.11}	F1	En este campo se indica el propósito del uso del certificado cualificado y el modulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En este caso se identifica que corresponde a un certificado emitido en modulo software y se debe indicar F1, en mayúscula.

Common Name (CN) {OID: 2.5.4.3}	ROBERTO DANIEL MACHADO FERNANDEZ	Este campo debe contener el/los nombre/s y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. No podrá ser incluido el uso de diéresis.
Serial Number {OID: 2.5.4.5}	CI1240596	CI más Número de Cédula de Identidad del titular del certificado, según documento de identificación
GivenName (G) {OID: 2.5.4.42}	ROBERTO DANIEL	Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. No podrá ser incluido el uso de diéresis.
Surname (SN)	MACHADO FERNANDEZ	Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. No podrá ser incluidos el uso de diéresis.

La estructura del certificado, referente a la extensión nombre alternativo del sujeto del certificado, es la que se describe como ejemplo en la siguiente tabla:

NOMBRE ALTERNATIVO DEL SUJETO del Certificado Cualificado Tributario F1		
Campo	**Valor de Ejemplo**	**Descripcion**
Rfc822Name	Roberto.machado@gmail.com	Email del titular del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.13}	description = FIRMA ELECTRONICA de nivel medio	En el caso para certificado del tipo F1 debe contener "FIRMA ELECTRONICA de nivel medio" Campo obligatorio.
DirectoryName {OID: 2.5.4.10}	O = FINESA S.A.	Nombre de la organización en el que presta servicio el titular del certificado. Campo obligatorio.
DirectoryName {OID: 2.5.4.11}	OU = AREA COMERCIAL	Nombre de la unidad de la organización en el que presta servicio el titular del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.5}	SerialNumber = RUC8167151-3	RUC seguido más el Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado. Campo obligatorio.

DirectoryName {OID: 2.5.4.12}	T = GERENTE COMERCIAL	Cargo o Titulo del titular del certificado. Campo no obligatorio

Los otros campos que compone la extensión "Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuando estén aprobados por la AC Raíz-Py Descripción del resto de campos más relevantes del perfil certificado cualificado Tributario F1:

Campo	Componente Propuesto	Critica
Versión	V3	
Serial Number	[NÚMERO DE SERIE DEL CERTIFICADO DIGITAL. VALOR ÚNICO EMITIDO DENTRO DEL ÁMBITO DE LA AC DE CONFIRMA S.A.]	
Signature Algorithm	sha256RSA	
Signature Has Algorithm	shA256	
Issuer	C = PY O = CONFIRMA S.A. CN = CA- CONFIRMA S.A. SERIALNUMBER = RUC80113823-0	
Validez	[PUEDE SER HASTA 1 AÑO]	
Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits o 4096 bits	
Certificate Policies . Policy Identifier . URL	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.58404.1.2.1.1 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS	NO

DPC . Notice Referente	Certificador: https://www.confirma.com.py/repositorio-confirma/ [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado cualificado de firma electrónica tipo F1 (claves en módulo software), sujeta a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de CONFIRMA S.A.	
CRLDistribution Points	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl1.confirma.com.py/public/pki/crl/confirma.crl [2]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl1.confirma.com.py/public/pki/crl/confirma.crl	NO
Auth. Information Access . CAIssuers . OCSP	Se utilizará http://ocsp1.confirma.com.py/public/pki/ocsp/	NO
KeyUsage	Firma Digital (Digital Signature) Cifrado de Clave (Key Encipherment) No Repudio (Non Repudiation)	SI
extKeyUsage	Autenticación del servidor (1.3.6.1.5.5.7.3.1) Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)	NO
Subject Key Identifier	SHA-1 hash de la clave pública	NO
Autority Key Identifier	debe contener el hash SHA-1 de la clave pública del PCSC	NO
Basic Contraints	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno	SI

7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PCSC de CONFIRMA S.A., según su PC, implementan la versión 3 (tres) del certificado definido en la norma ITU X.509 de acuerdo con el perfil establecido en la RFC 5280.

7.1.2. EXTENSIONES DEL CERTIFICADO

La ICPP define las siguientes extensiones como obligatorias:

a) Identificador de la clave de la Autoridad Certificadora "Authority Key Identifier", no crítica: El campo key Identifier debe contener el hash SHA-1 de la clave pública del PCSC;

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

c) Uso de Claves "Key Usage", crítica:

c.1.3) para certificados cualificados tributarios: debe contener los bits digitalSignature, keyEncipherment o keyAgreement y nonRepudiation activados.

d) Uso Extendido de la Clave "Extended Key Usage", no crítico:

para certificados cualificados tributarios:el propósito *client authentication OID =1.3.6.1.5.5.7.3.2* debe estar activado. Puede contener el propósito *server authentication OID = 1.3.6.1.5.5.7.3.1.*

e) Directivas del Certificado "Certificate Policies" no crítica:

e3)_**para certificados cualificados tributarios:**

e.3.1)_el campo ***policyIdentifier*** debe contener los OIDs de la PC implementada por el PCSC titular del certificado, para la emisión de certificados de personas físicas;

e.3.2) el campo **policyQualifiers**

e.3.2.1) elcamp**o *CPS Pointer*** debe contener la dirección web de la DPC del PCSC que emite el certificado.
e.3.2.2) el campo ***User Notice*** debe decir:"**certificado cualificado de firma electrónica tipo** [*siglas:* **F1 (claves en módulo software), F2 (claves en dispositivo cualificado) o F3 (claves en dispositivo cualificado centralizado)** *según tipo de certificado*] sujeta a las condiciones de uso expuestas en la DPC del PCSC CONFIRMA S.A."

f) **Restricciones Básicas *Basic Constraints*", crítica:**
f.1) el campo ***Subject Type*** debe contener Entidad Final= True
f.2) el campo ***PathLenConstraint*** debe tener valor cero;

g) Puntos de distribución de las LCR "CRL Distribution Points", no crítica:
g.1) el campo ***Distribution Point 1*** debe contener la primera dirección web donde se obtiene la LCR correspondiente al certificado; y
g.2) el campo ***Distribution Point 2*** debe contener la segunda dirección web donde se obtiene la LCR correspondiente al certificado.

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

h.1) Primer acceso

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

h.1.2) en el campo ***Access Location 1*** debe contener la dirección Web del servicio del OCSP, utilizando uno de los siguientes protocolos de acceso: HTTP, HTTPS o LDAP.

h.2) Segundo acceso

h.2.1) en el campo ***Access Method 2*** debe contener el identificador de método de acceso del certificado del PCSC; y

h.2.2) en el campo ***Access Location 2*** debe contener la dirección web donde se encuentra alojado el certificado del PCSC, utilizando uno de los siguientes protocolos de acceso: HTTP, HTTPS o LDAP.

i) **Nombre Alternativo del Sujeto "Subject Alternative Name", no crítica**, en los siguientes formatos:

i.3) Para CERTIFICADO CUALIFICADO TRIBUTARIO:
i.3.1) Campo NO obligatorio: Rfc822Name= [*email del titular del certificado***]**;
i.3.2) 3 (tres) campos otherName, obligatorios, que contienen:

1. **DirectoryName OID= 2.5.4.10: [***nombre de la organización en la que presta servicio el titular del certificado o razón social del titular del certificado en caso de tratarse de una organización unipersonal***]**;

2. **DirectoryName OID=2.5.4.5: RUC [**siglas **RUC** seguido del *número de RUC correspondiente a la organización en la que presta servicio el titular del certificado o el numero de RUC del titular del certificado en cas de tratarse de una organización unipersonal***]**;

3. **DirectoryName OID=2.5.4.13:** *debe contener el siguiente mensaje***:**
3.1) para certificado del tipo F1: [''FIRMA ELECTRÓNICA de nivel medio''] *o;*
3.2) para certificado del tipo F2: [''FIRMA ELECTRÓNICA CUALIFICADA''] *o;***3.3) para certificado del tipo F3: [''FIRMA ELECTRÓNICA CUALIFICADA CENTRALIZADA'']**
i.3.3) 2 **(dos) campos otherName, NO obligatorios, que contienen:**
1. **DirectoryName OID= 2.5.4.11: [nombre de la unidad de la organización en el que el presta servicio el titular del certificado***n***]**; y

2. **DirectoryName OID=2.5.4.12: [posición o función designada al titular del certificado en la organización en el que presta servicio]**;
Los campos otherName definidos por la ICPP deben cumplir con las siguientes especificaciones:

a) El conjunto de información definido en cada campo otherName debe almacenarse como una cadena de tipo **ASN.1 OCTET STRING o PRINTABLE STRING**; y

b) Solo se pueden utilizar los caracteres de la A a la Z, del 0 al 9, observando lo establecido en el ítem 7.1.5 del presente documento.

Otros campos que componen la extensión "**Subject Alternative Name**" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280 siempre y cuando estén aprobados por la AC Raíz-Py.

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS

Los certificados del PCSC de CONFIRMA S.A. deberán ser firmados utilizando el algoritmo definido en el documento DOC-ICPP-06.

7.1.4. FORMAS DEL NOMBRE

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

Certificado cualificado tributario:

i) OID=2.5.4.6 C=PY

ii) OID=2.5.4.10 O= CERTIFICADO CUALIFICADO TRIBUTARIO

iii) OID=2.5.4.11 OU= [F1*]*

iv) OID:2.5.4.3 CN= [*nombre/s y apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**; y

v) OID: 2.5.4.5. Serial Number= [conforme *al formato descripto en el ítem 3.1.4.2 del documento DOC-ICPP-03 [3]***]**;

vi) OID: 2.5.4.4 SN= [*apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**; y

vii) OID:2.5.4.42 GN= [*nombre/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**;

7.1.5. RESTRICCIONES DEL NOMBRE

Los certificados emitidos bajo esta política cuentan con DN conforme a las recomendaciones X.509 que son únicos y no ambiguos.

Los nombres deberán escribirse tal y como figuran en el documento de identificación presentado.

La ICPP establece las siguientes restricciones de nombres, aplicables a todos los certificados:

a) no se deben utilizar tildes ni diéresis; y
b) además de los caracteres alfanuméricos, sólo se podrán utilizar los siguientes caracteres especiales:

Tabla 4 - Caracteres especiales permitidos en los nombres

Caracteres	Código (hexadecimal)
Blanco	20
!	21
"	22
#	23
$	24

%	25
&	26
'	27
(	28
)	29
*	2A
+ ,	2B 2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

?	3F
@	40
\	5C

7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

Los OID asignados a las políticas de certificación contenidas en este documento se indican en el apartado 1.2.

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

Este Ítem no aplica.

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

En los certificados emitidos por el PCSC de CONFIRMA S.A. según su PC, el campo ***policyQualifiers*** de la extensión Políticas de certificado "Certificate Policies", contiene la dirección web (URL) de la DPC del PCSC responsable.

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

En el certificado emitido por el PCSC de CONFIRMA S.A. es una extensión crítica y deben ser interpretadas conforme a la RFC 5280.

7.2. PERFIL DE LA LCR

Como establezca la DPC del PCSC CONFIRMA S.A.

7.2.1 NÚMERO (S) DE VERSIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

Como establezca la DPC del PCSC CONFIRMA S.A.

7.3. PERFIL DE OCSP

Como establezca la DPC del PCSC CONFIRMA S.A.

7.3.1. NÚMERO (S) DE VERSIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

7.3.2. EXTENSIONES DE OCSP

Como establezca la DPC del PCSC CONFIRMA S.A.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

En los apartados siguientes se refieren a los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A o deben ser detallados los aspectos específicos para la PC si los hubiere.

8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

8.2. IDENTIFICACIÓN/CALIFICACIÓN DEL EVALUADOR

Como establezca la DPC del PCSC CONFIRMA S.A.

8.3. RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Como establezca la DPC del PCSC CONFIRMA S.A.

8.4. ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

Como establezca la DPC de CONFIRMA S.A.

8.6. COMUNICACIÓN DE RESULTADOS

Como establezca la DPC de CONFIRMA S.A.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

En los apartados siguientes se refierena los ítems correspondientes de la DPC del PCSC de CONFIRMA S.A o deben ser detallados los aspectos específicos para la PC si los hubiere.

9.1. TARIFAS

9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.1.1. TARIFAS DE ACCESO A CERTIFICADOS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.1.2. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

9.1.3. TARIFAS POR OTROS SERVICIOS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.1.4. POLÍTICAS DE REEMBOLSO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.2. RESPONSABILIDAD FINANCIERA

9.2.1. COBERTURA DE SEGURO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.2.2. OTROS ACTIVOS

Este ítem no aplica

9.2.3. COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

Como establezca la DPC del PCSC CONFIRMA S.A.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.2. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Como establezca la DPC del PCSC CONFIRMA S.A.

9.3.3. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Como establezca la DPC del PCSC CONFIRMA S.A.

9.3.4. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.2. INFORMACIÓN TRATADA COMO PRIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

9.4.8. INFORMACIÓN A TERCEROS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.5. DERECHO DE PROPIEDAD INTELECTUAL

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DEL PCSC

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.1. AUTORIZACION PARA CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.2. PRECISIÓN DE LA INFORMACION

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.3. IDENTIFICACION DEL SOLICITANTE

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.5. SERVICIO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.6. REVOCACION

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.1.7. EXISTENCIA LEGAL

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA AR

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.3. REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.4. REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.6.5. REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Como establezca la DPC del PCSC CONFIRMA S.A.

9.7. EXENCIÓN DE GARANTÍA

Como establezca la DPC del PCSC CONFIRMA S.A.

9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL

Como establezca la DPC del PCSC CONFIRMA S.A.

9.9. INDEMNIZACIONES

Como establezca la DPC del PCSC CONFIRMA S.A.

9.10. PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

La PC entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AC Raíz-Py.

9.10.2. FINALIZACIÓN

La presente PC permanecerá en vigencia indefinidamente, siendo válida y efectiva hasta que sea revocada o sustituida, expresa o tácitamente.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

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

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Como establezca la DPC del PCSC CONFIRMA S.A.

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

El procedimiento para enmiendas y que propuestas de modificación de la PC del PCSC de CONFIRMA S.A son revisadas y aprobadas por la AC Raíz-Py antes de ser implementadas. Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Toda enmienda o modificación de la PC, deberá ser publicada en el repositorio del PCSC de CONFIRMA S.A.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Como establezca la DPC del PCSC CONFIRMA S.A.

9.14. NORMATIVA APLICABLE

Como establezca la DPC del PCSC CONFIRMA S.A.

9.15. ADECUACIÓN A LA LEY APLICABLE

Como establezca la DPC del PCSC CONFIRMA S.A.

9.16. DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

Los titulares o responsables de certificados y las partes usuarias que confían en los certificados asumen en su totalidad el contenido de la presente PC.

Esta PC representa las obligaciones y deberes aplicables al PCSC de CONFIRMA S.A. y autoridades vinculadas.

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

9.16.2. ASIGNACIÓN

Como establezca la DPC del PCSC CONFIRMA S.A.

9.16.3. DIVISIBILIDAD

Como establezca la DPC del PCSC CONFIRMA S.A.

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

Como establezca la DPC del PCSC CONFIRMA S.A.

9.16.5. FUERZA MAYOR

Como establezca la DPC del PCSC CONFIRMA S.A.

9.17. OTRAS DISPOSICIONES

Como establezca la DPC del PCSC CONFIRMA S.A.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS EXTERNAS

- ● RFC 5280: "Internet X.509 Public Key Infrastructure.Certificate and Certificate Revocation List (CRL) Profile".

  ● RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

  ● TU X.500/ISO 9594: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".

  ● ITU X.509/ISO/IEC9594-8:"-Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".

  ● Principles and Criteria for Certification Authorities.

  ● WebTrustSM/TM Principles and Criteria for Registration Authorities.

  ● LEY N° 6822/2021 " "DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS."

  ● DECRETO N° 7576/2022 POR EL CUAL SE REGLAMENTAN ARTÍCULOS DE LA LEY N° 6822/2021,"DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS".

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla No 5 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CODIGO
[1]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[2]	Procedimientos operacionales mínimos para el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico. DOC-ICPP-07	DOC-ICPP-07
[3]	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
[4]	Directivas obligatorias para la formulación y elaboración de	DOC-ICPP-04

	la política de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	

10.3. INDICE DE TABLAS