DIGITO
FIRMA DIGITAL

POLITICA DE CERTIFICACIÓN
CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

Versión: 1.1

Año 2022

documenta sociedad anonima

CONTROL DOCUMENTAL

DOCUMENTO	
Título:	Política de Certificación de Certificado Cualificado de Firma Electrónica
Fecha:	04/08/2022
Versión:	1.1
Código:	PCSC-DOC-PCFEV1.1
Ubicación física:	Documenta S.A.
Soporte lógico:	https://www.digito.com.py

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
1.1	04/08/2.022	Primera Versión

DISTRIBUCION DEL DOCUMENTO	
Nombre	**Área**
PCSC Documenta S. A	Todas las Áreas
AR vinculadas a PCSC Documenta S.A.	Todas las Áreas
AV vinculadas a PCSC Documenta S.A.	Operadores
Ministerio de Industria y Comercio	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
DOCUMENTO PÚBLICO Y GRATUITO https://www.documenta.com.py	

Preparado	**Verificado**	**Aceptado**
JAVIER DÁVALOS Jefe Operaciones y Productos Documenta S.A.	**ROBERTO FRETES** Supervisor Operaciones Dígito Documenta S.A.	**JOSE ORICCHIO URRUTIA** Presidente Documenta S.A.

Contenido

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que obligatoriamente deberá cumplir el Prestador Cualificado de Servicio de Confianza (PCSC) DOCUMENTA S.A. en su carácter de Autoridad de Certificación Intermedia (ACI) y como integrante de la Infraestructura de Clave Pública del Paraguay (ICPP), para la formulación y la elaboración de su política de certificación (PC).

Toda PC elaborada en al ámbito de la ICPP debe obligatoriamente adoptar la misma estructura empleada de este documento.

Los tipos de certificados "F" 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.

Esta PC es aplicable a los siguientes certificados:

- Certificado cualificado de Firma Electrónica
  - F2

El par de claves criptográficas relacionadas a los tipos de certificado F2 deberán obligatoriamente ser generados y almacenados en módulos criptográficos tipo hardware en un:

- dispositivo Smart Card con capacidad de generación de claves; o
- token criptográfico u otro dispositivo equivalente, con capacidad de generación de claves.
- Módulo de seguridad hardware (HSM).

Las claves privadas relacionadas con los certificados del tipo F2 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 de Firma Electrónica
Versión del documento	1.1
Fecha de aprobación	04/08/2022
Localización	https://www.digito.com.py
OID (Object Identifier)	1.3.6.1.4.1.48315.1.1.1.10.1

1.3. PARTICIPANTES DE LA ICP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados electrónicos y de la asignación a sus titulares. Así mismo, efectúan la revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas. A las entidades autorizadas a emitir certificados de clave pública dentro de la ICPP se denominan:

- Autoridad Certificadora Raíz del Paraguay (AC Raíz): emite certificados a los PCSC bajo la jerarquía del Certificado Raíz. El certificado raíz es un certificado auto-firmado, en el que se inicia la cadena de confianza. Subordinados al Certificado Raíz, se encuentran los certificados emitidos al PCSC. En el Paraguay, la cadena de certificación tiene como máximo dos niveles, en el primer nivel se encuentra la AC Raíz, en el segundo nivel, uno o varios PCSC, éstos solo podrán emitir certificados electrónicos a usuarios finales. Se constituye como AC Raíz del Paraguay el MIC.
- Autoridad Certificadora Intermedia (CAI): Es la persona jurídica que emite certificados electrónicos a usuarios finales. En el ámbito de la ICPP un PCSC es considerada una CAI.

El PCSC DOCUMENTA S.A. es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, cuenta con un certificado electrónico emitido por la AC Raíz-Py y solo podrá emitir certificados a usuarios finales.

- Autoridad Certificadora Raíz del Paraguay (AC Raíz-Py): En la cúspide de la Jerarquía de la Infraestructura de Clave Pública del Paraguay (ICPP), se ubica la AC Raíz-Py, la misma cuenta con un certificado auto emitido y aceptado por los terceros que confían en la ICPP. Emite certificados a los PCSC y a partir de allí, comienza la cadena de confianza. Los certificados electrónicos emitidos por la AC Raíz-Py se rigen y ajustan a su Declaración de Prácticas de Certificación (DPC), cuyo cumplimiento es de carácter obligatorio.
- Autoridad Certificadora Intermedia (ACI): Es una entidad habilitada por la Autoridad de Aplicación (AA), encargada de operar una AC en el marco de la ICPP, debe contar con un certificado electrónico emitido por la AC Raíz-Py y solo podrá emitir certificados a personas físicas y jurídicas. En el ámbito de la ICPP un PCSC es considerado una ACI.

Un PCSC presta servicios de creación, verificación y validación de firmas electrónicas cualificadas y/o sello electrónico cualificado y certi0ficados relativos a estos servicios.

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

El PCSC DOCUMENTA S.A., una vez habilitado para brindar servicios de generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello, deberá utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación se utilicen bajo el control exclusivo del

titular del certificado. Además, deberá custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

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

1.3.2. AUTORIDADES DE REGISTRO (AR)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de los procesos de recepción, identificación y remisión de solicitudes de emisión o revocación de certificados electrónicos y de identificación de sus solicitantes.

DOCUMENTA S.A. cumple funciones de AR. Además, podrá mediante un acuerdo operacional establecer Autoridades de Registros Delegadas siempre y cuando las mismas estén autorizadas por la AC Raíz con la habilitación correspondiente.

Los datos referentes a las AR habilitadas por DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.digito.com.py/autoridades-de-registro

El PCSC DOCUMENTA S.A. mantiene publicada en el sitio las siguientes informaciones actualizadas:

- Lista de todas las AR habilitadas;
- para cada RA, las direcciones de todas las instalaciones técnicas, autorizadas por la AC Raíz-Py para funcionar;
- acuerdos operacionales celebrados entre el PCSC DOCUMENTA S.A. y una AR delegada; y
- la lista de todas las AR cuya habilitación fue revocada, con la indicación de la fecha de revocación.

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

Son entidades propias o externas a las que recurre la AC mediante un acuerdo operacional autorizado por la AC Raíz-Py con la habilitación correspondiente para suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por la AC.

Las informaciones actualizadas de las VA habilitadas por el PCSC DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.digito.com.py/autoridades-de-validacion en donde se publica:

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

1.3.4. TITULARES DEL CERTIFICADO

Se definen como aquellas personas físicas o jurídicas que podrán ser titulares de los certificados emitidos por el PCSC según corresponda a un certificado cualificado de firma electrónica, tributario o de sello electrónico cualificado respectivamente conforme a esta DPC.

1.3.5. PARTE USUARIA

Se entenderá por parte usuaria, toda persona física o jurídica, diferente al titular del certificado que decide aceptar y confiar en un certificado electrónico emitido dentro de la ICPP.

Una parte usuaria puede o no, ser un titular de certificado.

1.3.6. OTROS PARTICIPANTES

1.3.6.1 PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

PSS son entidades externas a las que recurre la AC o la AR mediante un acuerdo operacional autorizado por la AC Raíz-Py con la habilitación correspondiente para desempeñar actividades descritas en esta DPC o en una PC y se clasifican en tres categorías, conforme al tipo de actividades prestadas;

A) disponibilización de infraestructura física y lógica;

B) disponibilización de recursos humanos especializados; y

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

Las informaciones actualizadas de las PSS habilitadas por el PCSC DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.digito.com.py/prestadores-de-servicios

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

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

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

A continuación, las PC a las que aplica este documento:

Política	OID
Política de Certificación de Certificado Cualificado de Firma Electrónica V.1	1.3.6.1.4.1.48315.1.1.1.10.1

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

DOCUMENTA 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 Cualificados de Firma Electrónica F2 serán utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de integridad de sus informaciones.

TIPO	DESCRIPCIÓN DE USO APROPIADO
Certificado Cualificado de Firma Electrónica tipo F2	Firma Digital y Autenticación ● No repudio (Non- Repudiation) ● Firma Digital (Digital Signature) ● Cifrado de Clave (Key Encipherment)

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los Certificados Cualificados de Firma Electrónica F2 no deben emplearse para actividades especificadas como prohibidas en la normativa vigente, la DPC o en esta PC.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PCSC: DOCUMENTA S.A.

1.5.2. PERSONA DE CONTACTO

Nombre: JEFE OPERACIONES Y PRODUCTOS DIGITO DE DOCUMENTA S.A.

Teléfono: 021 7290002

Página web: https://www.digito.com.py

E-mail: firmadigital@documenta.com.py

Dirección: Avda. Rca. Argentina 893 c/ Alberto de Souza, Asunción - Paraguay

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

Nombre: JEFE DE OPERACIONES Y PRODUCTOS

Teléfono: 021 7290002

E-mail: firmadigital@documenta.com.py

Dirección: Avda. Rca. Argentina 893 c/ Alberto de Souza, Asunción – Paraguay

La entidad competente para determinar la adecuación de esta DPC es el personal del PCSC DOCUMENTA S.A. con autorización del Directorio, conforme con los estatutos de la empresa. Además, según lo establecido en la normativa vigente, la AA será la encargada de determinar la adecuación de la DPC de los PCSC que formen parte de la ICPP.

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

El Directorio y el personal autorizado del PCSC DOCUMENTA S.A., conforme con los estatutos de la empresa, aprobaran el contenido de la DPC y sus posteriores enmiendas. Luego será puesta a consideración de la AA para su aprobación.

1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1) **Agente de registro**: persona responsable de la realización de las actividades inherentes a la AR. Es la persona que realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.
2) **Autenticación**: proceso técnico que permite determinar la identidad de una persona física o jurídica.
3) **Autenticación electrónica**: proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
4) **Autoridad de Aplicación**: Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
5) **Autoridad de Certificación**: entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la ICPP, son Autoridades de Certificación la AC Raíz-Py y el PCSC.
6) **Autoridad de Certificación Raíz del Paraguay**: órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
7) **Autoridad de Certificación Intermedia**: entidad cuyo certificado de clave pública ha sido emitido por la AC Raíz-Py; es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador Cualificados de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.
8) **Autoridad de Registro:** entidad responsable de la interfaz entre el usuario y el Prestador de Servicios de Certificación (PCSC). Siempre está vinculado a un PCSC y su función es recibir solicitudes de emisión o revocación de certificados electrónicos del solicitante, identificar de forma presencial al mismo y remitir la solicitud al PCSC. La AR puede ser propia del PCSC o delegada a un tercero. entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.

9) **Autoridad de Validación**: entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una autoridad de registro y certificados por la autoridad de certificación. La AV puede ser propia del PCSC o delegada a un tercero.
10) **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
11) **Cadena de certificación:** lista ordenada de certificados que contiene un certificado de usuario final y certificados de las AC, que termina en un certificado raíz. El emisor del certificado del usuario final 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 usuario final o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.
12) **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley Nº 6822/2021.
13) **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley Nº 6822/2021.
14) **Certificado cualificado tributario:** certificado expedido por un Prestador Cualificado de Servicios de Confianza, el cual podrá ser utilizado para todos los fines convencionales ante el Sistema 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.
15) **Cifrado**: es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.
16) **Cifrado asimétrico**: tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
17) **Contrato de prestación de servicio de confianza:** Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado que contiene información relativa al solicitante del certificado y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.
18) **Claves criptográficas**: valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
19) **Clave pública y privada**: la criptografía en la que se basa la ICPP, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y

está incorporada en el certificado electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular del certificado.

20) **Compromiso**: violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
21) **Data Center (Centro de Datos)**: infraestructura compuesta por el espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una AC, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados electrónicos emitidos por la AC.
22) **Datos de activación**: valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.
23) **Declaración de Prácticas de Certificación**: declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
24) **Documento de identidad**: documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión/revocación del certificado electrónico será considerada la cédula de identidad o el pasaporte del solicitante.
25) **Dossier de titular del certificado**: Conjunto formado por la verificación de los documentos de identificación utilizados para la emisión del certificado, solicitud de certificado y Contrato de Prestación de Servicios de Confianza, y por la solicitud de revocación, cuando sea el caso. Este dossier deberá estar en formato de archivo digital, en el cual se escanean los documentos en formato papel, si los hubiere y se firma la solicitud de certificado y Contrato de Prestación de Servicios de Confianza con la clave privada del titular, después de la autorización del AGR por medio de la firma de dichos documentos, siempre y cuando sea informado y aceptado su contenido por parte de su solicitante y firmada digitalmente después de la generación de las claves y anterior a la instalación del certificado correspondiente.
26) **Emisor del certificado**: persona jurídica cuyo nombre aparece en el campo emisor de un certificado.
27) **Emisión de certificado**: es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
28) **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control

exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

29) **Firmante:** una persona física que crea una firma electrónica.
30) **Generador**: máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la CA, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin, de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.
31) **Habilitación**: autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
32) **Identificador de Objeto**: sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.
33) **Identificación del Solicitante de certificado**: comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a través de la presencia física del interesado, con base en los documentos de identificación, y la etapa de emisión del certificado, conforme en la presente DPC.
34) **Infraestructura de Claves Públicas del Paraguay**: conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos y claves criptográficas emitidas por esta infraestructura.
35) **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
36) **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
37) **Lista de Confianza:** Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley Nº 6822/21.
38) **Módulo criptográfico:** software o hardware criptográfico que genera y almacenas claves criptográficas.
39) **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
40) **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.

41) **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley Nº 6822/2021.
42) **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley Nº 6822/2021.
43) **Parte usuaria:** es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido en el marco de la ICPP.
44) **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
45) **Política de Certificación:** documento en el cual la AC define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
46) **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
47) **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
48) **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.
49) **Registro de Auditoría**: registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.
50) **Repositorio**: sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
51) **Rol de confianza:** función crítica que desempeña personal de la AC, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la AC.
52) **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
53) **Solicitante de Certificado**: persona física o jurídica que solicita la emisión de un certificado a una AC.
54) **Solicitud de Firma de Certificado**: petición de certificado electrónico que se envía a la AC. mediante la información contenida en el CSR, la AC, puede emitir el certificado electrónico una vez realizadas las comprobaciones que correspondan.

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

1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AC	Autoridad de Certificación
AGD	Autoridad de Gestión de Datos
AGR	Agente de Registro
C	Country (C por su sigla en inglés, Country)
CAI	Autoridad de Certificación Intermedia
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CN	Nombre común (CN por sus siglas en inglés, Common Name)
PC	Políticas de Certificación

DPC	Declaración de Prácticas de Certificación
LCR	Lista de certificados revocados
CRL	Lista de certificados revocados (CRL por sus siglas en inglés, Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
DN	Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PAS	Pasaporte
PCN	Plan de Continuidad del Negocio
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Claves Públicas del Paraguay
OEC	Organismo de Evaluación de la Conformidad
PCSC	Prestador Cualificado de Servicios de Certificación
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte

Py	Paraguay
AR	Autoridad de Registro
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RUC	Registro único del Contribuyente
SN	Número de Serie (por sus siglas en inglés, Serial Number)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
AV	Autoridad de validación

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1 REPOSITORIOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 NOMBRES

3.1.1. TIPOS DE NOMBRES

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.1.5. UNICIDAD DE NOMBRES

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.1.6. PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.1.7. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Como establezca la DPC del PCSC DOCUMENTA 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 DOCUMENTA S.A.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

No aplica.

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.2.7 PROCEDIMIENTOS COMPLEMENTARIOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.2.8 PROCEDIMIENTOS ESPECÍFICOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DENUEVAS CLAVES

Como establezca la DPC del PCSC DOCUMENTA S.A.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Como establezca la DPC del PCSC DOCUMENTA 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 DOCUMENTA S.A.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA 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 DOCUMENTA S.A.

4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DEL CERTIFICADO ELECTRÓNICO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.6 RENOVACIÓN DEL CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA 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 PCSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

Este Ítem no aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

Este ítem no aplica.

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

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

Este ítem no aplica.

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Este ítem no aplica.

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

Este ítem no aplica.

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

Este ítem no aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.8 LATENCIA MÁXIMA PARA LCR

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.10 REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

Como establezca la DPC del PCSC DOCUMENTA 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 DOCUMENTA S.A.

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.9.16 LÍMITES DEL PERÍODO DE SUSPENSIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.10 SERVICIOS DE ESTADO DEL CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.10.2 DISPONIBILIDAD DEL SERVICIO

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.10.3 CARACTERÍSTICAS OPCIONALES

Como establezca la DPC del PCSC DOCUMENTA S.A.

4.11 FIN DE ACTIVIDADES

Como establezca la DPC del PCSC DOCUMENTA 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 DOCUMENTA 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

5.1 CONTROLES FÍSICOS

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.1.2 ACCESO FÍSICO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.1.2 ENERGÍA Y AIRE ACONDICIONADO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.1.3 EXPOSICIÓN AL AGUA

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

5.1.4 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.1.5 ALMACENAMIENTO DE MEDIOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.1.6 ELIMINACIÓN DE RESIDUOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.1.7 RESPALDO FUERA DE SITIO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.2 CONTROLES PROCEDIMENTALES

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.2.1 ROLES DE CONFIANZA

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3 CONTROLES DE PERSONAL

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

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

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.4.8 EVALUACIÓN DE VULNERABILIDADES

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.5 ARCHIVOS DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.5.2 PERÍODOS DE RETENCIÓN PARA ARCHIVOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.5.3 PROTECCIÓN DE ARCHIVOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Este ítem no aplica.

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.6 CAMBIO DE CLAVE

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Como establezca la DPC del PCSC DOCUMENTA S.A.

5.8 EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

Como establezca la DPC del PCSC DOCUMENTA S.A.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

Compete a la AC Raíz-Py el seguimiento de la evolución tecnológica y en caso necesario,

actualizar las normas y los algoritmos criptográficos utilizados en la ICPP.

Una persona física, éste 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.

Una persona jurídica, la persona física que se presenta como un representante autorizado de la persona jurídica será el responsable de generar el par de claves criptográficas, salvo en caso de su gestión en nombre del creador del sello, en donde las claves privadas asociadas a los certificados son generadas y custodiadas por el módulo de activación de sello del PCSC, de forma que el acceso a dichas claves se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del creador del sello.

El algoritmo a ser utilizado para las claves criptográficas de titulares de certificados, está definido en el documento DOC-ICPP-06[1].

Cuando es generada, la clave privada del titular del certificado 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 siguiente tabla:

Tipo de certificado	Medio de almacenamiento
F2	• Hardware criptografico certificado por el MIC (Tarjeta inteligente o token con capacidad de generacion de claves) • Hardware criptografico certificado por el MIC (HSM)

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 muestren 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 de un PCSC, en los términos establecidos en el documento DOC-ICPP-07[2]

6.1.2 ENTREGA DE LA CLAVE PRIVADA AL TITULAR

Ítem no aplicable. La generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Para la generación del CSR por el PCSC DOCUMENTA S.A., se adoptará el formato definido en el documento DOC-ICPP-06 [3].

Los procedimientos específicos aplicables deben ser detallados en cada PC implementada.

La clave pública del PCSC DOCUMENTA S.A. es entregada a la AC Raíz mediante la entrega de una solicitud de firma de certificado (CSR) en el formato definido en el documento DOC-ICPP-06 [3]

6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LAS PARTES QUE CONFÍAN

Las formas para la disponibilización del certificado del PCSC DOCUMENTA S.A., y de todos los certificados de la cadena de certificación, para los usuarios y las partes que confían de la ICPP, comprenden, entre otras:

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

6.1.5 TAMAÑO DE LA CLAVE

El tamaño de las claves para cada tipo de certificado emitido por el PCSC DOCUMENTA S.A. son definidos en base a los requerimientos aplicables establecidos en el documento DOC-ICPP-04 [1].

El tamaño de las claves del PCSC DOCUMENTA S.A. se definen en base a los requerimientos aplicables establecidos en el documento DOC-ICPP-06 [3].

6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

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

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

Los usos admitidos de la clave para los certificados cualificados de firma electrónica F2 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 F2 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

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

Este ítem no aplica

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

El PCSC DOCUMENTA S.A. no almacena ni copia las claves privadas de los titulares de certificados cualificados de firma electrónica (tipo F2).

6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

Cualquier persona física o jurídica, titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

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

6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

El PCSC no almacena las claves privadas asociadas a certificados de los tipos F2.

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 DOCUMENTA 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 LA 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.

6.2.10MÉTODO 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 DOCUMENTA 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 o sellos 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.

La siguiente tabla define el periodo máximo de validez:

Tipo de certificado	Tiempo de uso en años	Tiempo operacional en años	Periodo máximo de validez del certificado (en años)
F2	4	4	Emitido por un tiempo máximo de 4 (cuatro) año, al finalizar ese período pierde su validez.

6.4 DATOS DE ACTIVACIÓN

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para certificados cualificados de firma electrónica F2 la generacion y almacenamiento del par de claves son realizados en dispositivos criptográficos hardware, con capacidad de generacion de claves, siendo activados y protegidos por contraseñas o PIN y/o identificación biométrica.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Se garantiza que los datos de activación de la clave privada del PCSC DOCUMENTA S.A. son protegidos contra el uso no autorizado, por medio de mecanismos de criptografía y de control de acceso físico.

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

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulaciones

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Como establezca la DPC del PCSC DOCUMENTA 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 DOCUMENTA S.A.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.6.4 CONTROLES EN LA GENERACIÓN DE LCR

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1 DIRECTRICES GENERALES

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.7.2 FIREWALL

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Como establezca la DPC del PCSC DOCUMENTA S.A.

6.8 FUENTES DE TIEMPO

Como establezca la DPC del PCSC DOCUMENTA S.A.

7. PERFILES DE CERTIFICADOS, LCR Y OCSP

7.1 PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PCSC DOCUMENTA S.A. cumplen con 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 de firma electrónica F2 emitidos por la PCSC DOCUMENTA S.A.

Certificado Cualificado de Firma Electrónica F2

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 de Firma Electrónica F2		
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 DE FIRMA ELECTRONICA	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y se debe indicar CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA, en mayúscula y sin tilde.
Organization Unit (OU) {OID: 2.5.4.11}	F2	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 hardware y se debe indicar FIRMA F2, en mayúscula.
Common Name (CN) {OID: 2.5.4.3}	JAVIER ARMANDO DOMINGUEZ TALAVERA	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}	CI8426243	CI o PAS del número de identificación, según documento de identificación
GivenName (G) {OID: 2.5.4.42}	JAVIER ARMANDO	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)	DOMINGUEZ TALAVERA	Este campo debe contener el/los apellido/s

{OID: 2.5.4.4}		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	javierdominguez@hmail.com	Email del titular del certificado. **Campo no obligatorio.**
DirectoryName {OID: 2.5.4.13}	description = FIRMA ELECTRONICA CUALIFICADA	En el caso para certificado del tipo F2 debe contener "FIRMA ELECTRONICA CUALIFICADA". **Campo obligatorio**
DirectoryName {OID: 2.5.4.10}	O = BLANCO S.A.	Nombre de la organización en el que presta servicio el titular del certificado. **Campo no obligatorio.**
DirectoryName {OID: 2.5.4.11}	OU = AREA TECNICA	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 = RUC800561-3	RUC seguido más el Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado. **Campo no obligatorio**
DirectoryName {OID: 2.5.4.12}	T = DIRECTOR TECNICO	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 de Firma Electrónica F2:

Campo	**Componente Propuesto**	**Critica**
Versión	V3	
Serial Number	**[NÚMERO DE SERIE DEL CERTIFICADO DIGITAL. VALOR**	

	ÚNICO EMITIDO DENTRO DEL ÁMBITO DE LA CA DE DOCUMENTA S.A.]	
Signature Algorithm	sha256RSA	
Signature Has Algorithm	shA256	
Issuer	C = PY O = DOCUMENTA S.A. CN = CA-DOCUMENTA S.A. SERIALNUMBER = RUC80050172-1	
Validez	**[PUEDE SER HASTA 4 AÑOS]**	
Subject Public Key Info	**Algoritmo: RSA Encryption** **Longitud: 2048 bits o 4096 bits**	
Certificate Policies . Policy Identifier . URL DPC . Notice Referente	**[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.48315.1.1.1.10.1** **[1,1]Información de certificador de directiva:** **Id. de certificador de directiva=CPS** **Certificador:** **https://www.digito.com.py/descargas** **[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 F2 (claves en dispositivo cualificado), sujeta a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de DOCUMENTA S.A.**	NO
CRLDistributionPoints	**[1]Punto de distribución CRL** **Nombre del punto de distribución:** **Nombre completo:** **Dirección URL=https://www.digito.com.py/crl/documenta_ca.crl** **[2]Punto de distribución CRL** **Nombre del punto de distribución:** **Nombre completo:** **Dirección** **URL=https://www.documenta.com.py/digito/documenta_ca.crl**	NO
Auth. Information Access . CAIssuers . OCSP	**Se utilizará** https://www.digito.com.py/uploads/certificado-documenta-sa-1535117771.crt https://www.digito.com.py/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 DOCUMENTA S.A. implementa la versión 3 (tres) del estándar ITU X.509.

7.1.2 EXTENSIONES DEL CERTIFICADO

Todas las extensiones de certificado utilizadas y su criticidad en los certificados emitidos por el PCSC DOCUMENTA S.A. son:

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

b) **Identificador de la clave de la persona física o jurídica 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 "KeyUsage", crítica:**

c.1.1) **para certificados cualificados de firma electrónica:** debe contener los bits *digitalSignature*, *keyEncipherment* y *nonRepudiation* activados;

c.1.2) **para certificados cualificados de sello electrónico:** debe contener los bits *digitalSignature*, *keyEncipherment* y *nonRepudiation* activados;

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:**

d.1) **para certificados cualificados de firma electrónica**: al menos uno de los propósitos *client authentication OID= 1.3.6.1.5.5.7.3.2 o E-mail protection OID = 1.3.6.1.5.5.7.3.4* debe estar activado y pudiendo implementar otros propósitos instituidos, siempre que sean verificables y previstos por el PCSC en su PC de acuerdo con el RFC 5280;

d.2) **para certificados cualificados de sello electrónico**: al menos uno de los propósitos *client authentication OID= 1.3.6.1.5.5.7.3.2 o E-mail protection OID = 1.3.6.1.5.5.7.3.4* debe estar activado y pudiendo implementar otros propósitos instituidos, siempre que sean verificables y previstos por el PCSC en su PC de acuerdo con el RFC 5280;

d.3) **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*.

d.4) **para certificados de firma de respuesta OCSP:** solamente el propósito *OCSPSigning OID = 1.3.6.1.5.5.7.3.9* debe estar presente;

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

e.1) **para certificados cualificados de firma electrónica:**

e.1.1) 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 o jurídicas;

e.1.2) el campo **policyQualifiers**

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

e.1.2.2) el campo ***User Notice*** debe decir: "**certificado cualificado de firma electrónica tipo** [*siglas:* **F2 (claves en dispositivo cualificado)** o **F3 (clave en dispositivo cualificado centralizado)** *según tipo de certificado*] sujeta a las condiciones de uso expuestas en la DPC del [*nombre del PCSC*]"

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

f.1) el campo ***Subject Type*** debe contener CA=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) Segunda entrada

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.1) Para CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA:

i.1.1) Campo NO obligatorio: Rfc822Name= [*email del titular del certificado***];**

i.1.2) 1 (un) campo otherName, obligatorio, que contiene:

1. **DirectoryName OID=2.5.4.13:** *debe contener el siguiente mensaje***:**

1.1) para certificado del tipo F2: [‘‘FIRMA ELECTRÓNICA CUALIFICADA’’*]*

1.2) para certificado del tipo F3: [‘‘FIRMA ELECTRÓNICA CENTRALIZADA CENTRALIZADA”*]*

i.1.2) 4 (cuatro) campos otherName, NO obligatorios, que contienen:

1. **DirectoryName OID= 2.5.4.10: [***nombre de la organización en el que presta servicio el titular del certificado***];**
2. **DirectoryName OID= 2.5.4.11: [***nombre de la unidad de la organización en el que presta servicio el titular del certificado***];**
3. **DirectoryName OID=2.5.4.5: RUC [**siglas **RUC** seguido del *número de RUC correspondiente a la organización en el que presta servicio el titular del certificado o el número de RUC del titular del certificado si no se registran los datos de la organización en la que presta servicio***];**
4. **DirectoryName OID=2.5.4.12: [***posición o función designada al titular del certificado en la organización en el que presta servicio o titulo académico del titular del certificado****];**

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 **(tres) campos otherName, NO obligatorios, que contienen:**

1. **DirectoryName OID= 2.5.4.11: [***nombre de la unidad de la organización en el que presta servicio el titular del certificado***];**
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 ALGORÍTMOS

Los certificados del PCSC DOCUMENTA S.A. deberán ser firmados utilizando el algoritmo definido en el documento DOC-ICPP-06 [3].

7.1.4 FORMAS DEL NOMBRE

El nombre del PCSC DOCUMENTA S.A., que consta el campo "Subject", deberá adoptar el "Distinguished Name" (DN) del estándar ITU X.500/ISO 9594 de la siguiente forma:

a) **Certificado cualificado de firma electrónica**:

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

ii) **OID=2.5.4.10 O=CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA**;

iii) **OID=2.5.4.11 OU= [***podrá ser:* **F2 o F3,** *conforme lo estipulado en el punto 1.1 y 1.4.1 de este documento***]**;

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 G= [** *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 identidad 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:

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)

Dirección Web (URL) de la PC y de la DPC aplicables: https://www.digito.com.py/descargas

Los certificados emitidos bajo estos documentos deben contener, en el campo policyQualifiers de

la extensión Políticas de certificado “Certificate Policies” estas informaciones.

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

Las extensiones críticas deben interpretarse de acuerdo con RFC 5280.

7.2 PERFIL DE LA LCR

Como establezca la DPC del PCDC DOCUMENTA S.A.

7.2.1 NÚMERO (S) DE VERSIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

7.2.2 LCR Y EXTENSIONES DE ENTRADAS DE LCR

Como establezca la DPC del PCDC DOCUMENTA S.A.

7.3 PERFIL DE OCSP

Como establezca la DPC del PCDC DOCUMENTA S.A.

7.3.1 NÚMERO (S) DE VERSIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

7.3.2 EXTENSIONES DE OCSP

Como establezca la DPC del PCDC DOCUMENTA S.A.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

8.2 IDENTIDAD/CALIDAD DEL EVALUADOR

Como establezca la DPC del PCDC DOCUMENTA S.A.

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Como establezca la DPC del PCDC DOCUMENTA S.A.

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

Como establezca la DPC del PCDC DOCUMENTA S.A.

8.6 COMUNICACIÓN DE RESULTADOS

Como establezca la DPC del PCDC DOCUMENTA S.A.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

Este ítem no aplica.

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.1.4 TARIFAS POR OTROS SERVICIOS

Este ítem no aplica.

9.1.5 POLÍTICAS DE REEMBOLSO

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

Como establezca la DPC del PCDC DOCUMENTA 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 PCDC DOCUMENTA S.A.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Este ítem no aplica.

9.4.8 INFORMACIÓN A TERCEROS

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.5 DERECHO DE PROPIEDAD INTELECTUAL

Según legislación vigente.

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PCSC

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Aplicase conforme al ítem 4 de esta DPC.

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Este ítem no aplica.

9.7 EXENCIÓN DE GARANTÍA

Este ítem no aplica.

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.9 INDEMNIZACIONES

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.9.1 PLAZO

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.9.2 FINALIZACIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.9.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.10 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.11 ENMIENDAS

9.11.1 PROCEDIMIENTOS PARA ENMIENDAS

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.11.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.11.3 CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.12 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.13 NORMATIVA APLICABLE

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.14 ADECUACIÓN A LA LEY APLICABLE

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.15 DISPOSICIONES VARIAS

9.15.1 ACUERDO COMPLETO

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.15.2 ASIGNACIÓN

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.15.3 DIVISIBILIDAD

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.15.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DEDERECHOS)

Este ítem no aplica

9.15.5 FUERZA MAYOR

Como establezca la DPC del PCDC DOCUMENTA S.A.

9.16 OTRAS DISPOSICIONES

Éste ítem no aplica.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS

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

- WebTrust Principles and Criteria for Certification Authorities.
- WebTrustSM/TM Principles and Criteria for Registration Authorities.

10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-04
[2]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación del PCSC que genera o gestiona datos de creación de firma electrónica y/o de sello electrónico.	DOC-ICPP-07
[3]	Procedimiento de identificación del solicitante de certificados por videoconferencia en la ICPP	DOC-ICPP-17
[4]	Características mínimas de seguridad para las autoridades de registro de la ICPP.	DOC-ICPP-05
[5]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[6]	Guía para la acreditación de los organismos de evaluación de la conformidad	DOC-ICPP-11
[7]	Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP	DOC-ICPP-12
[8]	Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP	DOC-ICPP-14
[9]	Directrices de la Política tarifaria de la AC Raíz-Py	DOC-ICPP-13