| **DOCUMENTO** | |
|---|---|
| **Titulo:** Declaración de Practicas de Certificación de la CA de Documenta S. A. | **Soporte lógico:** https://www.documenta.com.py/firmadigital/descargas |
| **Fecha:** 05/11/20015 | **Ubicación física:** Documenta S.A |
| **Código :** PKIpy-DocSA-CPSv1.0.0 | |
| **Versión:** 1.0.0 | |

| **REGISTRO DE CAMBIOS** | | |
|---|---|---|
| **Versión** | **Fecha** | **Motivo del cambio** |
| 1.0.0 | 05/11/2015 | Primera versión del documento |

| **DISTRIBUCION DEL DOCUMENTO** | |
|---|---|
| Nombre | Área |
| CA de Documenta S. A | Todas las Áreas |
| RA de Documenta S. A | Todas las Áreas |
| Sede Administrativa Documenta S. A. | Todas las Áreas |
| DOCUMENTO PÚBLICO Y GRATUITO | |

| **Preparado** | **Revisado** | **Aprobado** | **Aceptado** |
|---|---|---|---|
| | | | |
| Consultora | Coordinador de Seguridad | Gerente General Documenta S. A | Presidente Directorio |

# Contenido

# 1. INTRODUCCION

## 1.1. Descripción General

La expedición de certificados electrónicos a entidades que deseen actuar como Autoridades de Certificación subordinadas o Prestadoras de Servicios de Certificación emitiendo certificados digitales bajo la jerarquía del Certificado de la Autoridad Certificadora Raíz del Paraguay (CA del Paraguay), requerirá de una habilitación del Ministerio de Industria y Comercio (MIC), como autoridad de aplicación (AA) de Ley N° 4017/2010 su Decreto Reglamentario Nº 7.369/2011 y la Ley N° 4610/2012.

Dichas normativas establecen la validez jurídica de la Firma Electrónica, la Firma Digital, los mensajes de datos y el expediente electrónico y regula la utilización de estas herramientas así como el funcionamiento de las Prestadoras de Servicios de Certificación, sus requisitos y obligaciones.

El Ministerio de Industria y Comercio como ente regulador debe:

- Administrar la Autoridad Certificación Raíz del Paraguay.
- Dictar las normas que regulen el Servicio de Certificación Digital en el País.
- Habilitar a los Prestadores de Servicios de Certificación.
- Auditar a los Prestadores de Servicios de Certificación.
- Revocar la habilitación de los Prestadores de Servicios de Certificación.
- Imponer sanciones a los Prestadores de Servicio de Certificación.

El Ministerio de Industria y Comercio tiene entre sus cometidos la administración de la Autoridad Certificadora Raíz del Paraguay. Dicha Autoridad Certificadora es la raíz de toda la Jerarquía de PKI, cuenta con un certificado autoafirmado y aceptado por los terceros que establezcan confianza en la PKI del Paraguay.

El Ministerio de Industria y Comercio como AA de la normativa vigente habilita la operación de los Prestadores de Servicios de Certificación (PSC) en la República del Paraguay, de esta manera los PSC habilitados pasan a ser parte de la cadena de confianza de la Infraestructura de Clave Pública del Parguay.

Este documento recoge la Declaración de Prácticas de Certificación (CPS por sus siglas en ingles) de DOCUMENTA S. A.,

que estipula el funcionamiento y operaciones como Prestador de Servicios de Certificación (PSC) dentro de la PKI del Paraguay.

La presente CPS se ha estructurado teniendo en cuenta las recomendaciones de la (Request for comments) RFC 3647 "Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF. Con el propósito de facilitar la lectura y análisis del documento se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase "No estipulado" en las secciones para las que no se haya previsto nada.

Todos los certificados que se emite dentro de la PKI del Paraguay son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

Esta CPS es específicamente aplicable a:

- Prestador de Servicios de Certificación (PSC).
- Usuario Final.
- Parte que confía.

## 1.2. Nombre e Identificación del documento

| | |
|---|---|
| **Nombre del documento** | **Declaración de Prácticas de Certificación de DOCUMENTA S. A.** |
| **Versión del documento** | **1.0.0** |
| **Estado del documento** | **Versión inicial** |
| **Fecha de emisión** | **01/09/2015** |
| **Fecha de expiración** | **No aplicable** |
| **OID (Object Identifier)** | |
| **Ubicación de la CPS** | https://www.documenta.com.py/firmadigital/descargas/cps.pdf |

## 1.3. Participantes de la PKI

Las entidades y personas intervinientes en la PKI son las que se enumeran a continuación:

1. Autoridades de Certificación (CA).
2. Autoridades de Registro (RA).
3. Solicitantes y Titulares de certificados.

4. Terceros que confían en los certificados de la PKI del Paraguay.
5. Otros Participantes.

### 1.3.1. Autoridades de Certificación (CA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la emisión de certificados digitales y de la asignación a sus titulares. Así mismo, efectúan la renovación y 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 PKI Paraguay se denominan:

- **Autoridad Certificadora Raíz del Paraguay (CA Raíz)** emite certificados a los PSC 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 PSC.

  En el Paraguay, la cadena de certificación tiene como máximo dos niveles, en el primer nivel se encuentra la CA Raíz, en el segundo nivel, uno o varios PSC, éstos solo podrán emitir certificados digitales a usuarios finales.
- **Prestador de Servicios de Certificación (PSC)** es la persona jurídica que emite firmas digitales y los certificados digitales para identificar el propietario y el estatus de dichas firmas.

  El PSC, una vez habilitado, pasa a ser parte de la cadena de confianza de la PKI Paraguay, y debe contar con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera una estructura jerárquica.

### 1.3.2. Autoridades de Registro (RA)

Son las personas, políticas, procedimientos y sistemas informáticos encargados de la 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) llevarán a cabo la identificación de los solicitantes de certificados conforme a las normas de esta CPS y el acuerdo suscrito con la CA.
La DGFD&CE y los PSC cumplen funciones de RA.
DOCUMENTA S.A. en su carácter de PSC habilitado, podrá establecer sucursales en todo el territorio de la república respecto a las funciones de Registro bajo su responsabilidad, cumpliendo las normas y procedimientos establecidos en la normativa vigente, previa comunicación y autorización de la AA. Para ello se establecerá convenios con otras entidades siempre bajo el control y supervisión de DOCUMENTA S. A.

### 1.3.3. Suscriptores

Se definen como entidades finales aquellas personas físicas sujetos de derechos, con capacidad suficiente para solicitar y obtener un certificado digital de la CA de DOCUMENTA S. A. a título propio o en su condición de representante de una persona jurídica.
A los efectos anteriores tendrán la consideración de Entidades Finales:

- **Solicitante:** cuando un ciudadano interesado en obtener un certificado, llena el formulario de solicitud estipulado por la CA de DOCUMENTA S. A., adquiere la condición de Solicitante. La mera solicitud de un certificado no implica la concesión del mismo, la cual queda supeditada al éxito del procedimiento de Registro ante el Puesto habilitado para el efecto, previa verificación de los atributos cuya certificación se solicita.
  Sólo las personas mayores de edad podrán solicitar y, en su caso, obtener certificados digitales emitidos por CA de DOCUEMENTA S. A.
- **Titular**: toda persona física o jurídica a quien se emite un certificado digital, dentro de la jerarquía PKI Paraguay.

### 1.3.4. Terceros que confían

En el ámbito de esta CPS, los Terceros que confían son las personas o entidades diferentes del titular que deciden

aceptar y confiar en los certificados emitidos por la CA de DOCUMETA S. A. dentro de la jerarquía PKI Paraguay.

### 1.3.5. Otros Participantes

No estipulado

## 1.4. Uso de los certificados

### 1.4.1. Usos apropiados del Certificado

Las Políticas de Certificación de 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 se describen los usos apropiados del Certificado de la CA raíz y del PSC DOCUMENTA S. A.

| TIPO | DESCRIPCIÓN DE USO APROPIADO |
|---|---|
| **Certificado de CA Raíz** | Firma de Certificado a PSC.<br>Firma de CRL de PSC.<br>• Firma de Certificado (Certificate Signing).<br>• Firma CRL sin conexión (Off line CRL Signing). |
| **Certificado de la CA de Documenta S. A.** | Firma de Certificado a sus suscriptores.<br>Firma de CRL de sus suscriptores.<br>• Firma de Certificado (Certificate Signing).<br>• Firma de CRL (CRL Signing). |

### 1.4.2. Usos prohibidos del certificado

Los certificados deben emplearse de acuerdo con las funciones y finalidades definidas en su correspondiente PC, sin que puedan utilizarse para otras tareas y otros fines no contemplados en aquella.

## 1.5. Administración de las Políticas

### 1.5.1. Organización que administra el documento

| | |
|---|---|
| **Nombre** | DOCUMENTA S. A. |
| **Dirección** | Avda. General Máximo Santos N°698<br>Asunción - Paraguay |
| **Código Postal** | 1429 |
| **Teléfono** | +59521492501/3 |

| | |
|---|---|
| **Correo electrónico** | firmadigital@documenta.com.py |
| **Página Web** | www.documenta.com.py |

### 1.5.2. Persona de Contacto

| | |
|---|---|
| **Nombre** | GERENTE GENERAL DE DOCUMENTA S. A. |
| **Dirección** | Avda. General Máximo Santos N°698 Asunción - Paraguay |
| **Código Postal** | 1429 |
| **Teléfono** | +59521492503/3 |
| **Correo electrónico** | fdgerencia@documenta.com.py |

### 1.5.3. Persona que determina la adecuación de la CPS a la Política

El Director General de Firma Digital y Comercio Electrónico del MIC, será el encargado de determinar la adecuación de la CPS de DOCUMENTA S. A.

### 1.5.4. Procedimientos de aprobación de declaración de Política de Certificación (CPS)

El MIC aprobará el contenido de la Declaración de Practicas de Certificación de DOCUMENTA S. A. y sus posteriores enmiendas o modificaciones.

## 1.6. Definiciones y acrónimos

### 1.6.1. Definiciones

**Acuerdo de Suscriptores:** Es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita tanto del PSC, como del suscriptor, respectivamente.

**Autenticación:** Proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste, y al cual se le vincula. Éste proceso no otorga certificación notarial ni fe pública.

**Autoridad de Aplicación (AA):** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital

y Comercio Electrónico, dependiente del Viceministerio de Comercio. Órgano Regulador competente designado por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 "De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico".

**Autoridad Certificadora (CA):** Entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de una RA y VA. En el marco de la PKI Paraguay, son Autoridades Certificadoras, la CA Raíz del Paraguay y el PSC.

**Autoridad Certificadora Raíz (CA Raíz):** Es la Autoridad de Certificación Raíz de la PKI Paraguay, cuya función principal es habilitar al PSC y emitirle certificados digitales. Posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza.

**Autoridad de Registro (RA):** Entidad responsable de la identificación y autenticación de titulares de certificados digitales, la misma no emite ni firma certificados. Una RA puede ayudar en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA, no necesita ser un organismo separado sino que puede ser parte de la CA.

**Certificado Digital (CD):** Es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.

**Cifrado asimétrico:** Tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionados.

**Claves criptográficas:** Valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

**Clave Privada:** Es una de las claves de un sistema de criptografía asimétrico que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

**Clave Pública:** Es la otra clave del sistema de criptografía asimétrica, que es usada por el destinatario de un mensaje

de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

**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 a las claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

**Declaración de Prácticas de Certificación (CPS):** Declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.

**Delta CRL:** Partición del CRL, dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.

**Emisión:** Comprende la generación, validación y firma de los Certificados; el proceso de generación es una función de la Autoridad de Registro, la validación y firma, función de la CA.

**Emisor del certificado:** Organización cuyo nombre aparece en el campo emisor de un certificado.

**Encriptación:** Proceso para convertir la información a un formato más seguro. Se convierte mediante un proceso matemático a un formato codificado, es decir ininteligible.

**Estándares Técnicos Internacionales:** Requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

**Firma Digital:** Es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

**Huella digital (Código de verificación o resumen):** Secuencia de bits de longitud fija obtenida como resultado

de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) el mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo (2) sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo (3) sea improbable, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

**Identificación:** Procedimiento de reconocimiento de la identidad de un solicitante o titular de certificado dentro de la jerarquía PKI Paraguay.

**Identificador de Objeto (OID):** Serie única de números enteros, que identifica inequívocamente un objeto de información.

**Infraestructura de Clave Pública (PKI):** Es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos.

**Integridad:** Característica que indica que un mensaje de datos o un documentos electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

**Lista de certificados revocados (CRL):** Lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

**Módulo criptográfico:** Software o Hardware criptográfico que genera y almacena claves criptográficas.

**Módulo de Seguridad de Hardware (HSM, Hardware Security Module):** Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

**No Repudio:** Refiere que la posesión de un documento electrónico y la firma digital asociada al mismo, será prueba efectiva del contenido y del autor del documento.

**Par de claves:** Son las claves privada y pública de un cripto sistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

**PKCS#10 (Certification Request Syntax Standard):** Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

**Parte que confía:** Es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos bajo la PKI Paraguay.

**Perfil del certificado:** Especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

**Periodo de operación**: Periodo de vigencia de un certificado, que comienza en la fecha y la hora en que es emitido por una CA, y termina en la fecha y la hora en que expira o se revoca el mismo.

**Periodo de uso:** Refiere al tiempo establecido para los certificados emitidos dentro la jerarquía de la PKI para determinados usos.

**Política:** Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

**Política de Certificación(CP):** Documento en el cual la CA, define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.

**Práctica:** Modo o método que particularmente observa alguien en sus operaciones.

Prestador de Servicios de Certificación (PSC): Entidad habilitada ante la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz y solo podrá emitir certificados a usuarios finales. 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 CA con el fin de difundir su información pública.

**Rol de confianza:** Función crítica que desempeña personal de la CA, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.

**Ruta del certificado:** Secuencia ordenada de certificados de entidades que, junto a la clave pública de la entidad inicial en la ruta, puede ser procesada para obtener la clave pública de la entidad final en la ruta.

**Servicio OCSP:** Permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.

**Solicitud de Firma de Certificado (CSR):** Es una petición de certificado digital que se envía a la CA. Mediante la información contendida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

**Suscriptor:** Persona física o jurídica titular de un certificado digital emitido por una CA.

**Usuario final:** Persona física o jurídica que adquiere un certificado digital de un PSC.

**Validez de la firma:** Aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado.

**Verificación de la firma:** Determinación y validación de: a) que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

**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.

### 1.6.2. Acrónimos

**C** País (del inglés, Country) Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**CA** Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority).

**CA Raíz** Autoridad Certificadora Raíz del Paraguay.

**CI** Cédula de identidad.

**CIE** Cédula de identidad extranjera.

**CDP** Punto de Distribución de CRL (Distribution Point).

**CN** Nombre común (del inglés, Common Name). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**CP** Políticas de Certificación (CP por sus siglas en inglés Certificate Policy).

**CPS** Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement).

**CRL** Lista de certificados revocados (CRL por sus siglas en inglés certifícate revocation list).

**CSR** Solicitud de firma de Certificado (CSR por sus siglas en inglés Certificate Signing Request) Conjunto de datos, que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública.

**DGFD&CE** Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio del Ministerio de Industria y Comercio.

**DN:** Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500.

**DNS** Servicio de nombre de dominio (DNS por sus siglas en inglés Domaine Name server).

**ETSI** Instituto Europeo de Normas de Telecomunicaciones (ETSI por sus siglas en inglés European Telecomunications Standards Institute).

**FIPS** Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés Federal Information Processing Standards).

**ISO** Organización Internacional para la Estandarización (ISO por sus siglas en inglés International Organization for Standardization).

**ITU-T** Unión Internacional de Telecomunicaciones – Sector de Normalización de las telecomunicaciones (ITU-T por sus siglas en inglés International Telecomunication Union – Telecomunication Standardization Sector)

**MIC** Ministerio de Industria y Comercio.
**O** Organización (del inglés Organization) Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
**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)
**PKI** Infraestructura de Clave Pública (PKI por sus siglas en inglés Public Key Infrastructure).
**PSC** Prestador de Servicios de Certificación.
**PY** Paraguay.
**RA** Autoridad de Registro (RA por sus siglas en inglés Registration Authority).
**RFC** Petición de Comentarios (RFC por sus siglas en inglés Request for Comments).
**RUC** Registro único del Contribuyente.
**SN** Número de Serie (del inglés, Serial Number)
**SSL** Capa de Conexión Segura (SSL por sus siglas en inglés Secure Sockets Layer).
**URL** Localizador uniforme de recursos (URL por sus siglas en inglés Uniform Resource Locator).

# 2. RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

## 2.1. Repositorios

El repositorio de la CA de DOCUMENTA S. A. está disponible durante 24 horas al día, 7 días a la semana. Consiste en un servicio Web de acceso libre. Dicho repositorio no contiene ninguna información de naturaleza confidencial.

## 2.2. Publicación de Información de Certificación

La CA de DOCUMENTA S. A. mantiene un repositorio en su sitio principal de internet que permite a las partes que confían verificar en línea la revocación de un Certificado y cualquier otra información necesaria para validar el estado del mismo.

La CA de DOCUMENTA S. A. mantiene publicada, entre otros aspectos la versión actualizada de:

| | |
|---|---|
| **Lista de certificados revocados CRL** | https://www.documenta.com.py/firmadigital/descargas/crldoc.crl |
| **Servicio de OCSP** | http://www.documenta.com.py/firmadigital/oscp |
| **CA Raíz del Paraguay** | https://www.documenta.com.py/firmadigital/descargas/caraizpy.crt |
| **Certificado de CA Documenta S. A.** | https://www.documenta.com.py/firmadigital/descargas/cadoc.crt |
| **CPS** | https://www.documenta.com.py/firmadigital/descargas/cps.pdf |
| **CP Persona física** | https://www.documenta.com.py/firmadigital/descargas/cpf.pdf |
| **CP Persona jurídica** | https://www.documenta.com.py/firmadigital/descargas/cpj.pdf |

Además se publican Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay.

## 2.3. Tiempo o frecuencia de Publicación

Las enmiendas o modificaciones de la CPS se publicarán de acuerdo con lo establecido en el punto 9.12 de este documento.

Las actualizaciones del Acuerdo de Suscriptores serán publicadas cuando sufran modificaciones.

La información de estados de certificado, es publicada de acuerdo con a lo dispuesto en el punto 4.9.7 de este documento.

Las demás informaciones mencionadas en el punto anterior, serán actualizadas lo más pronto posible y con un máximo de un día hábil desde que se dispongan o surjan modificaciones.

## 2.4. Controles de Acceso a los Repositorios

El acceso para la consulta de las CPS y CP es abierto, pero sólo la DOCUMENTA S. A. está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello, DOCUMENTA S. A. establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.

# 3. IDENTIFICACION Y AUTENTICACION

## 3.1. Nombres

### 3.1.1. Tipos de Nombres

Todos los titulares de certificados requieren un nombre distintivo (Distinguished Name) conforme con el estándar X.500.

A continuación se define el procedimiento de asignación del nombre distintivo para el certificado de la CA de DOCUMENTA S. A. dentro de la Infraestructura de Claves Públicas del Paraguay:

| Campo | Valor | Descripción |
|---|---|---|
| Country (C) | **PY** | Código de país es asignado de acuerdo al estándar ISO 3166 |
| Organization (O) | **DOCUMENTA S. A.** | Denominación o Razón Social de la Persona Jurídica habilitada como PSC |
| Common Name (CN) | **CA-DOCUMENTA S. A.** | CA + Nombre de la CA |
| Serial Number<br>{OID: 2.5.4.5} | **RUC 80050172-1** | RUC Número de Cédula Tributaria correspondiente al PSC. |

El procedimiento de asignación de los nombres distintivos a los suscriptores para cada uno de los tipos de certificados se encuentra definido en el documento de Política de Certificación de DOCUMENTA S. A que corresponda en cada caso. Dicha definición debe estar en consonancia con las directrices generales descritas en este capítulo de la CPS.

### 3.1.2. Necesidad de Nombres significativos

En todos los casos los nombres distintivos de los titulares de los certificados son significativos.

En cualquier supuesto el dotar a los nombres distintivos de significado viene dado por la política a tal efecto desarrollada y descrita en el documento de Política de Certificación de DOCUMENTA S. A. correspondiente al certificado en cuestión.

### 3.1.3. Anonimato o seudónimos de los suscriptores

A fin de dar cumplimiento efectivo al atributo de "No Repudio" característico de los Certificados de Firma Digital no se admite el anonimato. Asimismo, el Seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del Certificado.

### 3.1.4. Reglas para interpretación de varias formas de Nombres

La regla utilizada por la CA de DOCUMENTA S. A. para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

**Certificado de CA de DOCUMENTA S.A**

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

| Tipo de Documento | Prefijo | Formato |
|---|---|---|
| Cédula Tributaria – RUC | RUC | RUC 99999999-9 |

Los procedimientos de garantía de la unicidad para cada tipo de certificado están establecidos en la Política de Certificación de DOCUMENTA S. A. correspondiente.

### 3.1.5. Unicidad de los nombres

La CA de DOCUMENTA S. A. debe asegurar que el "nombre distintivo del sujeto" (subject distinguished name) es único dentro de la PKI Paraguay.

El conjunto de nombre distintivo (Distinguished Name) debe ser único y no ambiguo. El uso del número de cédula tributaria (RUC) en el "Serial Number (Número de Serie)" del certificado de DOCUMENTA S. A. garantiza la unicidad del mismo.

Los procedimientos de garantía de la unicidad para cada tipo de certificado están establecidos en la Política de Certificación de DOCUMENTA S. A. correspondiente.

### 3.1.6. Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto 9.13. Reclamaciones de esta CPS.

### 3.1.7. Reconocimiento, autenticación y rol de las marcas registradas

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros. En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

La PKI Paraguay no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas o instituciones y marcas registradas.

DOCUMENTA S. A. tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

## 3.2. Validación inicial de la identidad

### 3.2.1. Medio de prueba de posesión de la clave privada

En caso de que el par de claves sea generado por el solicitante del certificado, la posesión de la clave privada, correspondiente a la clave pública para la que solicita que se genere el certificado, quedará probada mediante el envío de la petición de certificado (CSR) en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por la DGFD&CE, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

Este procedimiento podrá ser modificado por el que establezca en cada caso la Política de Certificación aplicable.

### 3.2.2. Autenticación de la identidad de una persona jurídica

En caso de que sea aplicable, cada CP establecerá el procedimiento de autenticación de la identidad de una persona jurídica.

En cada CP se establecerá la información a proporcionar por el solicitante, determinándose entre otros aspectos los siguientes:

- Tipos de documentos válidos para la identificación.
- Procedimiento de identificación por la CA o RA de la persona jurídica.
- Necesidad de identificación presencial.
- Forma de acreditar la pertenencia a una determinada organización.

#### 3.2.3. Autenticación de la identidad de una persona física

En caso de que sea aplicable, cada CP establecerá el procedimiento de autenticación de la identidad de una persona física.

En cada CP se establecerá la información a proporcionar por el solicitante, determinándose entre otros aspectos los siguientes:

- Tipos de documentos de identidad válidos para la identificación.
- Procedimiento de identificación por la CA o RA del individuo.
- Necesidad de identificación presencial.

#### 3.2.4. Información no verificada sobre el solicitante

No se contempla la inclusión de información no verificada en los certificados emitidos por la CA de DOCUMENTA S. A.

#### 3.2.5. Comprobación de las facultades de representación

DOCUMENTA S. A. Determinará si el solicitante se encuentra apto para solicitar un tipo de certificado específico. Además, debe validará que el solicitante no posea impedimentos legales.

**En el caso de Certificados de Personas Físicas, validará:**

- Nombre y documento de identidad
- Mayoría de edad.

**En el caso que el solicitante sea Persona Jurídica debe verificará:**

- Nombre o razón social y Cédula Tributaria
- Nombre del representante legal y documento de identidad.

DOCUMENTA S. A. verificará la información suministrada por el solicitante contra los datos oficiales correspondientes.

#### 3.2.6. Criterios para operar con CA externas

Podrán ser reconocidos los Certificados Digitales Extranjeros de conformidad a la normativa vigente.

### 3.3. Identificación y autenticación para solicitudes de re emisión de claves

#### 3.3.1. Identificación y autenticación para re emisión de claves rutinaria

No se permite la re emisión de claves.

### 3.3.2. Identificación y autenticación para la re emisión de claves después de una revocación

No se permite bajo estas circunstancias, la re emisión de claves. Luego del procedimiento de Revocación, se debe solicitar la emisión de un nuevo certificado.

## 3.4. Identificación y autenticación para solicitudes de revocación

El proceso de identificación y autenticación individual se define por la Política de Certificación aplicable a cada tipo de certificado, debiendo ser como mínimo tan estricto como el aplicado en la solicitud inicial del certificado.

# 4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

## 4.1. Solicitud de certificados

### 4.1.1. Quién puede efectuar una solicitud

En cada Política de Certificación se concreta quién puede solicitar un certificado y la información que se debe suministrar en la solicitud. Asimismo, la CP establece los pasos que deben seguirse para llevar a cabo este proceso.

### 4.1.2. Proceso de Inscripción y responsabilidades

En general, es atribución de cada RA de DOCUMENTA S. A. dentro de la PKI Paraguay determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la Política de Certificación aplicable en cada caso. La Autoridad de Registro podrá autorizar o denegar la solicitud de certificación.

Las solicitudes de los certificados, una vez completadas, serán enviadas a C A de DOCUMENTA S. A. por la Autoridad de Registro correspondiente.

DOCUMENTA S. A. Tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad del solicitante.
- Validar la información suministrada en la solicitud de certificado (CSR).
- Informar al suscriptor de sus deberes y responsabilidades con respecto al uso de certificados.
- Emitir y entregar el Certificado de acuerdo con la información suministrada en la solicitud

Como regla general, todo solicitante que desee un certificado deberá:

- Cumplimentar el formulario de solicitud del certificado con toda la información que DOCUMENTA S. A. requiera para la emisión del mismo. Cabe destacar que no toda la información solicitada aparecerá en el certificado y que ésta será conservada, de manera confidencial.
- Entregar la solicitud del certificado, que incluye la clave pública, en el caso de que el par de claves lo haya generado el solicitante, a la RA correspondiente y el certificado se genere directamente a partir de la solicitud. En la correspondiente CP se establecerá el procedimiento de entrega.

La existencia del formulario de solicitud y en general el procedimiento de solicitud de certificados DOCUMENTA S. A queda definido en la Política de Certificación correspondiente a cada uno de los certificados.

## 4.2. Procesamiento de la Solicitud del Certificado

### 4.2.1. Realización de las funciones de identificación y autenticación

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado.

### 4.2.2. Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que DOCUMENTA S. A haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El procedimiento por el que se determina la naturaleza y la forma de realizar dichas comprobaciones se establece en la Política de Certificación correspondiente.

### 4.2.3. Plazo para la tramitación de las solicitudes de certificados

El tiempo de procesamiento del CSR (lapso de tiempo entre la solicitud emitida a la CA y la emisión del certificado del suscriptor) cualquiera sea el caso, será en el menor tiempo posible. Se establecerán plazos mínimos para la tramitación de las solicitudes de los certificados en las CP correspondientes.

## 4.3. Emisión de certificados

### 4.3.1. Actuaciones de la CA durante la emisión del certificado

La emisión del certificado implica la autorización definitiva de la solicitud por parte de la CA. Cuando DOCUMENTA S. A emita un certificado de acuerdo con una solicitud de certificación, efectuará las notificaciones que se establecen en el apartado del presente capítulo.

Todos los certificados iniciarán su vigencia en el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, cuando se den las causas que motiven la revocación del certificado.

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de certificados acogidos a las mismas.

#### 4.3.2. Notificación al solicitante de la emisión por la CA del certificado

Cada CP DE DOCUMENTA S. A establecerá el mecanismo de notificación mediante el que se informará al solicitante de la emisión de su certificado.

### 4.4. Aceptación del certificado

#### 4.4.1. Mecanismo de aceptación del certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto a la PKI Paraguay.

Los certificados que exijan la presentación de una identificación, requerirán la aceptación explícita del titular del certificado y el reconocimiento de que está de acuerdo con los términos y condiciones contenidos en el Acuerdo de Suscriptores., que rige los derechos y obligaciones entre la DOCUMENTA S. A. y el titular, y de que éste conoce la existencia de la presente Declaración de Prácticas de Certificación, que recoge técnica y operativamente los servicios de certificación digital prestados en el marco de la PKI Paraguay .

En la CP correspondiente se podrán detallar o ampliar la forma en que se acepta el certificado.

#### 4.4.2. Publicación del certificado por la CA

En cada PC se detallarán los repositorios de publicación del certificado.

#### 4.4.3. Notificación de la emisión del certificado por la CA a otras Autoridades

No se definen entidades externas que necesiten o requieran ser notificados a cerca de los certificados emitidos por la CA.

### 4.5. Par de claves y uso del certificado

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

Las responsabilidades y limitaciones de uso del par de claves y del certificado se establecerán en la correspondiente PC. En cualquier caso, el titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la CP y de acuerdo con lo establecido en los campos **'Key Usage'** y **'Extended Key Usage'** del certificado. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones

de uso, establecidas en la CPS y CP, y sólo para lo que éstas establezcan.
Tras la expiración o revocación del certificado, el titular dejará de usar la clave privada.

#### 4.5.2. Uso de la clave pública y del certificado por la parte que confía

Los Terceros que Confían sólo pueden depositar su confianza en los certificados para aquello que establezca la correspondiente CP y de acuerdo con lo establecido en el campo 'Key Usage' y 'Extended Key Usage' del certificado.
Los Terceros que Confían han de realizar las operaciones de clave pública de manera adecuada para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los mecanismos establecidos en esta CPS y en la correspondiente PC.
Asimismo, se adhieren a las condiciones de uso establecidas en dichos documentos.

### 4.6. Renovación de certificados sin cambio de claves

La renovación del certificado no está permitida por esta CPS, cuando un certificado requiera ser renovado debe solicitarse uno nuevo, de acuerdo con la sección 4.1 de esta CPS.

#### 4.6.1. Circunstancias para la renovación de certificados sin cambio de claves

No estipulado.

#### 4.6.2. Quién puede solicitar la renovación de los certificados sin cambio de claves

No estipulado.

#### 4.6.3. Tramitación de las peticiones de renovación de certificados sin cambio de claves

No estipulado.

#### 4.6.4. Notificación de la emisión de un nuevo certificado al titular

No estipulado.

#### 4.6.5. Forma de aceptación del certificado sin cambio de claves

No estipulado.

#### 4.6.6. Publicación del certificado sin cambio de claves por la CA

No estipulado.

#### 4.6.7. Notificación de la emisión del certificado por la CA a otras Autoridades

No estipulado.

### 4.7. Renovación de certificados con cambio de claves

La renovación con cambio de claves no está permitida por esta CPS, cuando un certificado requiera ser re-emitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de esta CPS.

#### 4.7.1. Circunstancias para una renovación con cambio de claves (re-emisión)de un certificado

No estipulado.

#### 4.7.2. Quién puede pedir la renovación de los certificados

No estipulado.

#### 4.7.3. Tramitación de las peticiones de renovación de certificados con cambio de claves

No estipulado.

#### 4.7.4. Notificación de la emisión de un nuevo certificado al titular

No estipulado.

#### 4.7.5. Forma de aceptación del certificado con las claves cambiadas

No estipulado.

#### 4.7.6. Publicación del certificado con las nuevas claves por la CA

No estipulado.

#### 4.7.7. Notificación de la emisión del certificado por la CA a otras

No estipulado.

### 4.8. Modificación de certificados

#### 4.8.1. Circunstancias para la modificación de un certificado

Cuando se requiera la modificación de la información contenida en un certificado debe revocarse y realizar una solicitud para un nuevo certificado, de acuerdo con la sección 4.1 de esta CPS.

#### 4.8.2. Quién puede solicitar la modificación de los certificados

No estipulado.

#### 4.8.3. Tramitación de las peticiones de modificación de certificados

No estipulado.

#### 4.8.4. Notificación de la emisión de un certificado modificado al titular

No estipulado.

#### 4.8.5. Forma de aceptación del certificado modificado

No estipulado.

#### 4.8.6. Publicación del certificado modificado por la CA

No estipulado.

#### 4.8.7. Notificación de la modificación del certificado por la CA a otras Autoridades

No estipulado.

### 4.9. Revocación y suspensión de certificados

#### 4.9.1. Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se invalida un certificado antes de su caducidad. El efecto de la revocación de un certificado es el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La revocación de un certificado impide el uso legítimo del mismo por parte del titular.

El proceso de solicitud de revocación se define en la Política de Certificación aplicable a cada tipo de certificado.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público. Al expirar el periodo de validez de un certificado revocado, éste dejará de estar incluido en la CRL.

Sin perjuicio de lo dispuesto en la normativa aplicable un certificado podrá ser revocado por:

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales contenidos en el

acuerdo de suscriptores, la CP asociada o de la presente CPS.

- Por fallecimiento, ausencia legalmente declarada, incapacidad total o parcial de la persona física.
- Insolvencia, liquidación, quiebra de una persona jurídica.
- Emisión defectuosa de un certificado debido a que:
  - No se ha cumplido un requisito material para la emisión del certificado.
  - La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
  - Existencia de un error de entrada de datos u otro error de proceso.
- El par de claves generado por un titular se revela como "débil".
- La información contenida en un certificado o utilizada para realizar su solicitud deja de ser correcta.
- Por orden formulada por el titular o por tercero autorizado.
- El certificado de una CA superior en la jerarquía de confianza del certificado es revocado.
- Por la concurrencia de cualquier otra causa especificada en la presente CPS o en las correspondientes Políticas de Certificación establecidas para cada tipo de Certificado.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez del mismo, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta CPS ni tendrá efectos retroactivos.

### 4.9.2. Quién puede solicitar la revocación

DOCUMENTA S. A. puede solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del titular o cualquier otro hecho determinante que recomendara emprender dicha acción.

Los titulares de certificados o para el caso de persona jurídica el representante legal, también podrán solicitar la revocación de sus certificados, debiendo hacerlo de acuerdo con las condiciones especificadas en el apartado 4.9.3.

Asimismo, la Autoridad Judicial Competente o un tercero presentando evidencia contundente del uso indebido del certificado, compromiso de la clave, fallecimiento del titular u otro motivo de revocación establecido en la normativa vigente.
Las distintas Políticas de Certificación podrán definir otros procedimientos de identificación que sean más rigurosos.

### 4.9.3. Procedimiento de solicitud de revocación

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.
De forma general y sin perjuicio de lo definido en las CP se establece que:

- Se comunicará al titular del certificado la revocación del mismo mediante correo electrónico.
- Tras la revocación del certificado el titular deberá cesar en el uso de la clave privada que se corresponda con aquel.
- La solicitud de revocación de un certificado recibida con posterioridad a su fecha de caducidad no será atendida.

La información a suministrar para solicitar la revocación de un certificado se establecerá a expensas de lo especificado en la correspondiente Política de Certificación.

### 4.9.4. Periodo de gracia de la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

### 4.9.5. Plazo en el que la CA debe resolver la solicitud de revocación

Cada CP establecerá el tiempo máximo para la resolución de una solicitud de revocación, si bien se establece como norma general que se haga en menos de 24 horas.

### 4.9.6. Requisitos de verificación de las revocaciones por los terceros que confían

La verificación de las revocaciones, ya sea mediante consulta directa de la CRL o protocolo OCSP, es obligatoria para cada uso de los certificados por los Terceros que Confían.
Los Terceros que Confían deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargar la

nueva CRL del repositorio de la CA de DOCUMENTA S. A. al finalizar el periodo de validez de la que posean. Las listas de revocación de certificados guardadas en memoria "caché", aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Cuando la CP de aplicación admita otras formas de divulgación de información de revocación, los requisitos para la comprobación de dicha información se especificarán en la propia CP.

### 4.9.7. Frecuencia de emisión de CRL

DOCUMENTA S. A. Publicará una nueva CRL en su repositorio en el momento en que se produzca cualquier revocación. En cualquier caso, DOCUMENTA S. A. Publicará una nueva CRL en su repositorio a intervalos no superiores a 24 horas, aunque no se hayan producido modificaciones en la CRL, es decir, aunque no se haya revocado ningún certificado desde la última publicación.

DOCUMENTA S. A. garantiza la disponibilidad de las CRL con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

### 4.9.8. Tiempo máximo entre la generación y la publicación de las CRL

Cada CP establecerá el tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio.

### 4.9.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados

DOCUMENTA S. A. proporciona un servidor web donde publica las CRL para la verificación del estado de los certificados que emite. Asimismo, existe una Autoridad de Validación de DOCUMENTA S. A. que, mediante el protocolo OCSP, permite verificar el estado de los certificados.

### 4.9.10. Requisitos de comprobación en línea de revocación

En el caso de recurrir a la Autoridad de Validación de DOCUMENTA S. A., el Tercero que Confía debe disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

### 4.9.11. Otras formas de divulgación de información de revocación disponibles

Algunas CP pueden admitir a otras formas de aviso de revocación, como los Puntos de Distribución de CRLs (CPS).

#### 4.9.12. Requisitos especiales de revocación de claves comprometidas

En el caso de compromiso de la clave privada de la CA de DOCUMENTA S. A. será notificado, en la medida posible, a todos los participantes de la PKI Paraguay, en especial a:

- Todos los suscriptores de certificados emitidos.
- Terceros que confían, los que se tenga conocimiento

Además la DOCUMENTA S. A. publicará el compromiso de su clave en su sitio principal de internet y procederá a la inmediata gestión de la revocación de su certificado y el de sus suscriptores. DOCUMENTA S. A., publicará el certificado revocado en el repositorio.

DOCUMENTA S. A., deberá notificar en un plazo de veinticuatro horas como máximo a la DGFD&CE respecto a circunstancias que produzcan el compromiso de sus claves o su imposibilidad de uso.

#### 4.9.13. Causas para la suspensión

No estipulado.

#### 4.9.14. Quién puede solicitar la suspensión

No estipulado.

#### 4.9.15. Procedimiento para la solicitud de suspensión

No estipulado.

#### 4.9.16. Límites del periodo de suspensión

No estipulado.

### 4.10. Servicios de información del estado de certificados

#### 4.10.1. Características operativas

DOCUMENTA S. A. dispone como mínimo de dos servicios que proporcionan información sobre el estado de los certificados emitidos por su CA:

- Publicación de las listas de revocación de certificados (CRL). El acceso a las CRL se realiza vía HTTPS.
- Servicio de validación en línea (Autoridad de Validación, VA) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560. Mediante el uso de este protocolo es posible obtener el estado actual de un certificado electrónico sin requerir las CRL.

#### 4.10.2. Disponibilidad del servicio

El servicio, en sus dos variantes, está disponible de forma ininterrumpida todos los días del año, tanto para los

Terceros que Confían como para los Titulares de los certificados u otras partes que los requieran.
DOCUMENTA S. A. garantiza la disponibilidad de las CRL con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

#### 4.10.3. Características adicionales

DOCUMENTA S. A. en ningún caso proporcionará un cliente OCSP para hacer uso del Servicio de validación en línea. Es responsabilidad de quien desee utilizar dicho servicio disponer de un Cliente OCSP que cumpla la RFC 2560.

### 4.11. Extinción de la validez de un certificado

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas recogidas en el apartado 4.9.1.
- Expiración de la vigencia del certificado.

### 4.12. Custodia y recuperación de claves

#### 4.12.1. Prácticas y políticas de custodia y recuperación de claves

DOCUMENTA S. A. no custodia claves de los suscriptores de ningún certificado, únicamente se mantienen respaldos de sus propias claves privadas de acuerdo con el Plan de Continuidad de Negocio.
Para los efectos del Plan de Continuidad de Negocio, las clave privada de la de la CA de DOCUMENTA S. A. está custodiada y respaldada bajo estrictas normas de seguridad, y almacenada en dispositivos criptográficos FIPS 140-2 nivel 3, que garantizan la no divulgación de las claves.

#### 4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

No estipulado.

# 5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

A fin de asegurar la confiabilidad y seguridad de sus operaciones como prestador de servicios de certificación, DOCUMENTA S. A. ha dispuesto e implantado controles de seguridad física y lógica en todas sus instalaciones, al igual que procedimientos de auditoría, tanto interna como independiente para el seguimiento y verificación del cumplimiento de las políticas, directivas y procedimientos en materia de seguridad.

## 5.1. Controles físicos

### 5.1.1. Ubicación física y construcción

La infraestructura de DOCUMENTA S. A. se encuentra ubicada en varios edificios que disponen de medidas de seguridad de control de acceso, de forma que sólo se permita la entrada en los mismos a personas debidamente autorizadas.

Los centros de datos donde se aloja la infraestructura tecnológica de DOCUMENTA S. A. cuentan con seis perímetros de seguridad física:

- Primer perímetro: acceso a las instalaciones de la CA (área de recepción)
- Segundo perímetro: acceso al área de procesos administrativos de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el primero.
- Tercer perímetro: acceso al área de operación de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo.
- Cuarto perímetro: acceso al área de operaciones críticas de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el tercero.
- Quinto perímetro: acceso al área de resguardo de documentos y dispositivos sensibles.
  Área interna al tercer perímetro
- Sexto perímetro: acceso al área de resguardo de clave privada. Área interna al cuarto perímetro.

Los centros de datos donde se aloja la infraestructura disponen de al menos, los siguientes elementos de seguridad física:

- Muros perimetrales Reforzados.
- Generación de energía redundante.
- Sistema ininterrumpible de energía.
- Sistema de UPS redundante.

- Doble acometida eléctrica.
- Sistema de enfriamiento de precisión redundante.
- Sistema de detección, extinción y supresión automática de fuego.
- Sistema de monitoreo de infraestructura.
- Sistema de tierras físicas y pararrayos.
- Suministro de energía eléctrica regulada y con protección.
- Sistema de aire acondicionado HVAC.
- Seguridad física 24/7 (subsistema de seguridad mediante guardias de seguridad).
- Sistema CCTV con grabación con movimiento.

### 5.1.2. Acceso físico

La infraestructura Tecnológica de la CA de DOCUMENTA S. A. está físicamente separada de cualquier otro sistema y su acceso dispone de varios niveles de control. Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro que posee al menos, dos de los siguientes tres requisitos de acceso:

- Tarjeta de proximidad.
- Lectura biométrica.
- Contraseña de acceso.

Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios humanos y técnicos.

### 5.1.3. Alimentación eléctrica y aire acondicionado

La infraestructura de DOCUMENTA S. A cuenta con:
Suministro eléctrico:

- PDU redundadas.
- Dispone de grupos electrógenos, redundados para aquellas circunstancias en las que se presente un déficit en la generación eléctrica o sean frecuentes y/o prolongados los cortes en el suministro eléctrico.
- UPS: permite mantener la alimentación ininterrumpida mediante baterías cuando falla el suministro o se produce una anomalía. Alta disponibilidad y redundancia de los equipos.
- Doble acometida eléctrica para los equipos.

Aire acondicionado:

- Sistema de enfriamiento de precisión redundante.
- Sistema de aire acondicionado HVAC.

### 5.1.4. Exposición al agua

La infraestructura de DOCUMENTA S. A cuenta con:

- Sistemas de control de humedad y temperatura, monitorizado a tiempo real.
- Sistemas de drenaje y piso elevado.

#### 5.1.5. Prevención y protección frente a incendios

Las salas donde se ubican los activos de la infraestructura Tecnológica de DOCUMENTA S. A. disponen de los medios adecuados (varios niveles de sistemas automáticos de detección y extinción de incendios) para la protección de su contenido contra incendios.

El cableado se encuentra en suelo falso o techo falso y se dispone de los medios adecuados (detectores en suelo y techo- para la protección del mismo contra incendios).

#### 5.1.6. Sistema de almacenamiento

La información se dispone en medios de forma segura, según la clasificación de la información en ellas contenidas. Los sistemas de almacenamiento se encuentras en diferentes locaciones, para eliminar el riesgo asociado a una única ubicación.

#### 5.1.7. Eliminación de residuos

Se ha adoptado una política de gestión de residuos que garantiza el almacenamiento seguro de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

#### 5.1.8. Copias de seguridad fuera de las instalaciones

Se dispondrá al menos de una copia en un lugar seguro, fuera de los Centros de Proceso de Datos de la Infraestructura Tecnológica de Claves Publicas de de la CA de DOCUMENTA S. A.

### 5.2. Controles de procedimiento

DOCUMENTA S. A. procura que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorías periódicas.

Asimismo, se ha diseñado una segregación de funciones, para evitar que una sola persona pueda conseguir el control total de la infraestructura.

#### 5.2.1. Roles de confianza (responsables del control y gestión de la PKI de DOCUMENTA S. A.)

Estos roles contemplan, al menos las siguientes responsabilidades:

- ***Coordinador de Seguridad:*** Debe llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobadas por la CA, controlar la formalización de los convenios entre el personal y la CA, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, debe cumplir y hacer cumplir las políticas de seguridad de la CA y debe encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Es el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls Debe comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a estos, asimismo debe resolver o hacer que resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. y es el encargado de la gestión y control de seguridad física, y de los movimientos de material fuera de las instalaciones de la CA
- ***Receptor de Registro:*** el mismo tendrá a su cargo realizar la validación de identidad inicial del Solicitante.
- ***Jefe de Área***: es el responsable de autorizar tecnológicamente la emisión de un certificado o la revocación del mismo. Bajo su control y supervisión el Receptor de Registro y el Oficial de Registro.
- ***Administrador de Sistemas:*** son encargados de la instalación y configuración de sistemas operativos y del mantenimiento y actualización de los programas instalados. Tiene capacidad para configurar, mantener los sistemas, pero sin acceso a los datos. Asimismo, deberán establecer y documentar los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Son responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación de la CA y asumen la gestión de los servicios de ruteamiento y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Son encargados de la instalación de hardware criptográfico de CA y de la eliminación del hardware criptográfico de CA de producción.

Responsables del mantenimiento o reparación de equipos criptográficos CA (incluida la instalación de nuevo hardware, firmware o software)

- ***Responsable del mantenimiento de la CA:*** se encarga de las tareas de ejecución y revisión de las copias de seguridad del sistema, asimismo debe velar para que se lleven a cabo las copias de seguridad local y del traslado de las mismas de acuerdo con lo establecido en la política de seguridad. Son responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Encargados de la gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios.
- ***Auditor Interno de la CA:*** son los responsables de las tareas de ejecución y revisión de auditoría interna del sistema. Esta auditoría interna debe realizarse de acuerdo con las normas y criterios de auditoría establecidos en la CP y la presente CPS. Además cuenta con la capacidad de acceder a los registros del sistema.
- ***Desarrollo de sistemas de la CA***: Son encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones.
- ***Funciones de gestión del ciclo de vida de claves criptográficas:*** Se distinguen los siguientes responsables para la gestión del ciclo de vida de las claves criptográficas:
  - ***Oficial de Seguridad:*** responsable de la Administración del token/HSM, establecimiento de la política de seguridad del token, inicialización del token y creación de usuarios.
  - ***Oficial de Backup:*** es el responsable del Token de Backup, establecimiento de la política de clonado y de la creación/transferencia de dominios de clonado.
  - ***Oficial de acceso remoto:*** es el responsable de establecer una conexión PED remota.
  - ***Usuario de Partición:*** es el encargado de la generación de claves, firma y cifrado/descifrado.

- **Oficial de Registro:** el mismo tendrá a su cargo realización del proceso de emisión y revocación del certificado del suscriptor.

### 5.2.2. Número de personas requeridas por tarea

Se requiere un mínimo de dos personas para realizar operaciones sobre la PKI. de la CA de DOCUMENTA S. A.
DOCUMENTA S. A. mantiene y ejecuta procedimientos de control rigurosos para asegurar la segregación de funciones.

### 5.2.3. Roles que requieren segregación de funciones

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos roles marcados como "incompatibles":

- Incompatibilidad entre el rol auditor interno de la CA y cualquier otro rol.
- Incompatibilidad entre el rol de Coordinador de Seguridad y Administrador de Sistemas.
- Incompatibilidad entre el rol de Coordinador de Seguridad y Oficial de Registro.
- Incompatibilidad entre el rol de Coordinador de Seguridad y Usuario de Partición.

Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

- La validación de información en aplicaciones de certificado y de solicitudes o información del suscriptor.
- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación.
- La emisión o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La emisión o destrucción de los certificados de la CA.
- La puesta en operación de la CA en producción.

## 5.3. Controles de personal

### 5.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

El personal que ejecuta tareas de confianza en la PKI de DOCUMENTA S. A, debe poseer cualificación y experiencia en entornos de servicios de certificación e infraestructura de clave pública. Adicional, el personal debe cumplir con los requerimientos de seguridad dispuestos en la Política de Seguridad de la Información y además deben:

- Haber demostrado capacidad para ejecutar sus deberes.
- Haber suscripto un acuerdo de confidencialidad y disponibilidad.
- No poseer otros deberes que puedan interferir o causar conflicto con los de la CA.
- No tener antecedentes de negligencia o incumplimiento de labores.
- No tener antecedentes penales.

### 5.3.2. Procedimientos de comprobación de antecedentes

DOCUMENTA S. A. cuenta con procedimientos para verificar la cualificación y experiencia del personal que ejecuta tareas de confianza. El procedimiento incluye:

- Confirmación de empleos anteriores.
- Título académico y cursos obtenidos.
- Verificación de conocimientos específicos.
- Verificación de antecedentes judiciales y policiales.

### 5.3.3. Requerimientos de formación

El personal de DOCUMENTA S. A. debe estar sujeto a una formación específica, incluida en el Plan Anual de Capacitación. La información debe incluir:

- Conceptos básicos de PKI.
- Seguridad lógica y física de la operación.
- Servicios prestados por la Autoridad de Certificación.
- Aspectos legales relativos a la prestación de servicios de certificación.
- Políticas de Certificación y Declaración de Prácticas de Certificación.
- Procedimientos de operación, administración y mantenimiento para cada rol específico.
- Gestión de incidencias.
- Procedimientos para la recuperación de la operación en caso de desastres, para cada rol específico.

### 5.3.4. Requerimientos y frecuencia de actualización de la formación

Se proveerá formación al personal de DOCUMENTA S. A. ante cambios tecnológicos o en los sistemas de seguridad, introducción de nuevas herramientas, modificación de procedimientos operativos, cambios en la CPS, CP u otros documentos relacionados al funcionamiento,

administración y/o gestión de la infraestructura de clave pública.

### 5.3.5. Frecuencia y secuencia de rotación de tareas

DOCUMENTA S. A. efectuará rotaciones de trabajo entre los distintos roles al menos una vez cada 3 años, con el objetivo de incrementar la seguridad y garantizar la continuidad, en caso de ausencia de alguno de los trabadores.

Antes de asumir las nuevas funciones, el personal debe recibir una capacitación y/o actualización de acuerdo al rol específico, que le permita cumplir con las tareas satisfactoriamente.

### 5.3.6. Sanciones por actuaciones no autorizadas

Las prácticas que deben cumplir el personal DOCUMENTA S. A. y el procedimiento sancionador que incumplan las mismas, son recogidas en el Reglamento Interno de DOCUMENTA S. A y de acuerdo a lo estipulado en el documento suscripto para los roles de confianza.

### 5.3.7. Requisitos de contratación de terceros

DOCUMENTA S. A. puede contratar personal externo, consultores o terceros, solamente si existe una relación claramente definida con el contratista y bajo las siguientes condiciones:

- Existe un contrato con cláusulas propias de los roles de gestión y estipula sanciones para las actuaciones no autorizadas.
- No posee personal disponible para los roles de gestión contratados.
- Los contratistas cumplen con los mismos requisitos expuestos en el punto 5.3.1.
- Finalizados los servicios, se dará de baja al usuario y se le revocarán los accesos.

### 5.3.8. Documentación proporcionada al personal

DOCUMENTA S. A. proporciona al personal toda la documentación y buenas prácticas de seguridad de la información necesarias para el correcto desempeño de sus tareas. Entre la documentación se encuentran:

- CP Y CPS.
- Procedimientos de instalación, operación, mantenimiento y gestión de la PKI de acuerdo al rol específico.
- Política de Seguridad de la Información.

- Plan de continuidad del negocio y recuperación de desastres.
- Gestión de incidencias.
- Otros que se consideren necesario.

## 5.4. Procedimientos de auditoría de seguridad

### 5.4.1. Tipos de eventos registrados

DOCUMENTA S. A. posee mecanismos para registrar, entre otros, los siguientes tipos de eventos:

El acceso (logon) a las herramientas de gestión de los componentes de la PKI.

- La solicitud de emisión y revocación de certificados, por parte de las Autoridades de Registro registrando tanto el tipo de acción a realizar y sus parámetros, como la identificación de la aplicación, administrador u operador de registro que solicita la acción.
- Las acciones realizadas por los elementos de la PKI. Entre ellas:
  - La generación o revocación de certificados.
  - La actualización de CRL y su publicación en los repositorios.
- Arranque y parada de los servicios online de los componentes de la PKI.
- Los avisos (warnings) y errores producidos en el procesado de una petición de certificación. Asimismo, se registrarán los avisos (warnings) y errores producidos por mecanismos internos de la CA (tales como publicación de certificados y CRL).
- Los intentos de acceso no autorizado a los componentes de la PKI, indicando la identificación de la persona que está realizando el intento.

En cada evento se registrará:

- El tipo de evento registrado.
- La fecha y hora en que se ha producido.
- La identificación del usuario o componente de la PKI que solicitó la acción que provocó el evento.
- El rol con el que actuó el usuario o componente de la PKI que solicitó la acción que provocó el evento.
- El resultado de la acción que provocó el evento.
- La descripción de la acción realizada.
- Los parámetros (contenido) de la solicitud de la acción que provocó el evento.

Toda esta información puede ser consultada:

- A través de las Consolas de Gestión de los componentes de la PKI, para lo cual deberá autenticarse como Auditor del Sistema.
- A través de la Consola de Administración del Colector centralizado de Eventos, accediendo con un usuario con permisos suficientes.

Los registros de auditoría no deben registrar las claves privadas de ninguna forma y los relojes del sistema de cómputo de la CA deben estar sincronizados con el horario oficial de la república del Paraguay para un registro exacto de los eventos.

### 5.4.2. Frecuencia de procesado de registros de auditoría

Los registros se analizarán al menos una vez al mes, en las auditorías periódicas de la PKI, y de manera manual cuando sea necesario.

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

El procesamiento del registro de auditoría consiste en una revisión de los registros y la documentación de los motivos para los eventos significativos, y todas las acciones deben ser documentadas.

Los registros de auditorías deben ser recuperados solamente por personal autorizado, ya sea por razones válidas del negocio o por seguridad.

### 5.4.3. Periodo de conservación de los registros de auditoría

La información generada en los registros de eventos se conserva:

- En la base de datos de la PKI, durante todo el periodo de vida de la PKI.
- En el sistema Colector de Eventos, de modo que sea accesible online durante 30 días y al menos diez años por medio de backups.

### 5.4.4. Protección de los registros de auditoría

La información de los registros de eventos se encuentra protegida por mecanismos de firma y cifrado en la Base de Datos. Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.

- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.
- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él. Esto permite guardar un registro de las operaciones realizadas y evita que se pierdan firmas electrónicas realizadas anteriormente por otros usuarios cuando se actualizan los datos.

### 5.4.5. Procedimientos de respaldo de los registros de auditoría

DOCUMENTA S. A. garantiza que en todo momento existirá una copia de seguridad de los registros de auditoría de la PKI.

### 5.4.6. Notificación al sujeto causa del evento

Cuando un evento es almacenado por el registro, no se requiere notificar al causante de dicho evento, a excepción de que el evento sea de índole accidental y resulta probable que pueda volver a ocurrir.

### 5.4.7. Sistema de recolección de información de auditoría (interno vs externo)

Los archivos de registro son almacenados en los sistemas internos, mediante una combinación de procesos automáticos y manuales ejecutados por las aplicaciones de la PKI.

## 5.5. Archivado de registros

### 5.5.1. Tipo de eventos archivados

DOCUMENTA S. A. conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, se deben archivar los siguientes datos:

- Durante el inicio de operaciones de DOCUMENTA S. A. como PSC:
  - La resolución de Habilitación emitida por la Autoridad de Aplicación
  - el CP y el CPS de DOCUMENTA S. A;
  - Cualquier acuerdo contractual para establecer los límites del PSC;
  - La configuración del sistema que requiere la CA de DOCUMENTA S. A.
- Durante la operativa del PSC:

- modificaciones o actualizaciones de cualquiera de los ítems anteriores.
- solicitudes de certificados o de revocación;
- documentación para autenticar la identidad del suscriptor;
- documentación de recepción y aceptación del certificado;
- documentación de recepción de dispositivos de almacenamiento de claves;
- todos los certificados y CRL (información de revocación) tanto emitidos o publicados;
- registros de auditoría;
- otros datos o aplicaciones para verificar el contenido de los archivos;
- cumplimiento de auditoría.

### 5.5.2. Periodo de conservación de registros

Toda la información y documentación relativa a los certificados se conservarán durante un mínimo de 10 años.

### 5.5.3. Protección del archivo

Los eventos de aplicativos están protegidos de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos. Así mismo, la documentación en papel que se genere con motivo de los procedimientos de la PKI, será almacenada de forma segura en las instalaciones DOCUMENTA S. A.

### 5.5.4. Procedimientos de copia de respaldo del archivo

DOCUMENTA S. A. mantiene procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguran la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación del PSC.

### 5.5.5. Requerimientos para el sellado de tiempo de los registros

Sin estipulaciones

### 5.5.6. Sistema de archivo de información (interno vs externo)

Todo el archivado de información se realiza de forma interna a la PKI de DOCUMENTA S. A.

### 5.5.7. Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Auditor, que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la PKI de DOCUMENTA S. A.

## 5.6. Cambio de claves

DOCUMENTA S. A. debe cambiar sus claves de acuerdo con el tiempo de uso y tiempo operacional de los certificados emitidos dentro de la PKI Paraguay, este cambio técnicamente implica la emisión de un nuevo certificado.

El tiempo operacional de un certificado coincide con el descripto en los campos de ‘’Válido desde’’ y ‘’Válido hasta’’ del mismo. El tiempo de uso refiere al establecido para los certificados emitidos por la jerarquía de la PKI para determinados usos, como se aprecia a continuación:

| Nivel de Jerarquía | Tiempo de uso en años | Tiempo operacional en años | Descripción |
|---|---|---|---|
| Certificado de Suscriptores | 2 | 2 | El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez |
| Certificado de PSC DOCUMENTA S. A. | 8 | 10 | El Certificado emitido al PSC tendrá: Un tiempo operacional de 10 años, que resulta de la suma del tiempo de uso de su certificado (8 años) más el tiempo de validez máximo del certificado de su suscriptor (2 años).Solamente durante el tiempo de uso de su certificado, el PSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional solo podrá firmar la CRL de usuarios o |

| | | | |
|---|---|---|---|
| | | | suscriptores |

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

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

DUCUMENTA S. A. tiene la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores emitidas por ella, se ajusta con el tiempo operacional de todos los niveles superiores.

## 5.7. Recuperación ante compromiso de clave o catástrofe

### 5.7.1. Procedimientos de gestión de incidentes y compromisos

DOCUMENTA S. A. tiene establecido un Plan de Contingencia que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por su PKI.

El Plan de Contingencia contempla, entre otros aspectos, los siguientes:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.

En el caso de que se produjera un compromiso de los datos de verificación de firma de la CA de DOCUMENTA S. A. informará a todos los titulares de certificados de su PKI y terceros que confían conocidos de que todos los certificados y listas de revocación de certificados firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio.

Si un PSC no puede ser reestablecida en una semana, entonces su clave se reportará como comprometida y

todos sus certificados serán revocados. En casos excepcionales, la DGFD&CE, puede otorgar extensiones para el PSC

### 5.7.2. Alteración de los recursos hardware, software y/o datos

Si los recursos hardware, software, y/o datos se alteran o se sospecha que han sido alterados se detendrá el funcionamiento de la PKI hasta que se restablezca la seguridad del entorno con la incorporación de nuevos componentes cuya adecuación pueda acreditarse. De forma simultánea se realizará una auditoría para identificar la causa de la alteración y asegurar que no vuelva a producirse.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

### 5.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

En el caso de compromiso de la clave privada del certificado de la CA de DOCUMENTA S. A., se procederá a solicitar al MIC su revocación inmediata. Cesando el servicio de emisión de Certificados a usuarios finales o suscriptores.

Se notificará a todos los suscriptores afectados de la revocación del certificado la CA de DOCUMENTA S. A. y se procederá a la revocación de todos los certificados emitidos.

### 5.7.4. Capacidad de continuidad del negocio después de un desastre

El sistema de Autoridad de Certificación de DOCUMENTA S. A. puede ser reconstruido en caso de desastre. Para llevar a cabo esta reconstrucción es necesario contar con:

- Un sistema con hardware, software y dispositivo Hardware Criptográfico de Seguridad similar al existente con anterioridad al desastre.
- Las claves de administrador de la Autoridad de Certificación de DOCUMENTA S. A.
- Una copia de respaldo de los discos del sistema anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la CA, incluidas sus claves privadas.

El almacenado, tanto de las tarjetas de acceso de los administradores de las CA como de las copias de los discos de sistema de cada CA, se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

## 5.8. Cese de una PSC o RA

La terminación de una PSC o RA puede producirse en los siguientes casos:

- Cuando se extinga el plazo de vigencia del certificado y no se haya solicitado un nuevo certificado.
- En el caso que el PSC finalice sus servicios y por lo tanto, deje de operar.
- Si se hallare comprometida la clave privada del PSC o se produjera un desastre que ocasionare daños a las instalaciones del mismo que causare la destrucción de la clave privada y su copia de respaldo, el PSC debe solicitar que se revoque su certificado.

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

- Publicar en su sitio principal de internet la fecha de suspensión de los servicios con al menos 60 días de anticipación.
- Publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese.
- Notificar a sus suscriptores por lo menos 30 días antes de la suspensión efectiva o cese de sus operaciones En dicha notificación se especificará la fecha de la cesación efectiva de actividades así como los motivos por los cuales se procede a tal cese.

Proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

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

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

El MIC a través de la DGFDyCE custodiará toda la información referida al cese de operación del PSC, además publicará el cese de actividades o finalización del servicio del PSC en su sitio principal de internet.

Asimismo, los certificados que continúen vigentes, podrán ser transferidos a otro prestador de servicios de certificación, previo consentimiento del firmante y por cuenta del prestador de servicios de certificación.

En el caso de que la Autoridad de Registro cese en el ejercicio de las funciones, transferirá los registros que mantenga a la CA DOCUMENTA S. A., mientras exista la obligación de mantener archivada la información, y de no ser así, ésta será destruida.

# 6. CONTROLES TÉCNICOS DE SEGURIDAD

En el ámbito de la presente CPS se especificarán los detalles concernientes a las claves de la autoridad de certificación de DOCUMENTA S. A. Los detalles relativos a las claves de los titulares de los certificados se podrán consultar en la Política de Certificación que corresponda en función del tipo de certificado.

## 6.1. Generación e instalación del par de claves

### 6.1.1. Generación del par de claves

Los pares de claves para los componentes internos de PKI de DOCUMENTA S. A., se generan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 que tiene instalados en sus sistemas. Los pares de claves para el resto de titulares se generan en función de lo estipulado en la Política de Certificación aplicable a cada certificado.

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por DOCUMENTA S. A. vienen definidos por la Política de Certificación que le sea de aplicación.

### 6.1.2. Entrega de la clave privada al titular

El método de entrega de la clave privada a sus titulares depende de cada certificado y será establecido en la Política de Certificación correspondiente a cada certificado.

### 6.1.3. Entrega de la clave pública al emisor del certificado

El método de entrega de la clave pública al emisor en los casos en que la genere el Titular dependerá de cada certificado y será establecido en la Política de Certificación correspondiente.

### 6.1.4. Entrega de la clave pública de la CA a los terceros que confían

La clave pública de las CA de DOCUMENTA S. A. está a disposición de los terceros que confían en el Repositorio de DOCUMENTA S. A. (ver apartado 2.1) sin perjuicio de que una CP pueda establecer mecanismos adicionales de entrega de dichas claves.

### 6.1.5. Tamaño de las claves

El tamaño de las claves de la Autoridad Certificadora DOCUMENTA S. A. es de 4096 bits.

El tamaño de las claves para cada tipo de certificado emitido por DOCUMENTA S. A viene definido por la Política de Certificación que le sea de aplicación.

### 6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de la CA de DOCUMENTA S. A. está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es RSA.

Los parámetros de generación de claves para cada tipo de certificado emitido por DOCUMENTA S. A. vienen definidos en la Política de Certificación que le sea de aplicación.

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por DOCUMENTA S. A. vienen definidos por la Política de Certificación que le sea de aplicación.

### 6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509 v3)

La Clave privada de la CA de DOCUMENTA S. A. podrá ser utilizado con el único propósito de:

- firmar los certificados de sus Suscriptores; y,
- Firmar la CRL correspondiente.

El valor del campo key usage para este certificado es:

- KeyCertsign=1;
- CRLSign=1.

Los usos admitidos de la clave para cada tipo de certificado emitido por la CA de DOCUMENTA S. A. vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por la CA de DOCUMENTA S. A contienen la extensión Key Usage definida por el estándar X.509 v3, la cual se califica como crítica. Asimismo, pueden establecerse limitaciones adicionales mediante la extensión Extended Key Usage.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por DOCUMENTA S. A.

## 6.2. Protección de la clave privada y controles de ingeniería de los módulos

### 6.2.1. Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por la CA de DOCUMENTA S. A. cumplen con la certificación FIPS 140-2 de nivel 3.

La puesta en marcha de una Autoridad de Certificación, teniendo en cuenta que se utiliza un módulo Criptográfico de seguridad (HSM), conlleva las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las claves de los intervinientes.
- Generación de las claves de la CA.

DOCUMENTA S. A. utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. DOCUMENTA S. A. únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Nivel 3.

### 6.2.2. Control multipersona (m de n) de la clave privada

La clave privada de la CA de DOCUMENTA S. A. se encuentra bajo control multipersona. Ésta se activa mediante la inicialización del software de CA por medio de la combinación mínima de operadores de la CA correspondiente. Éste es el único método de activación de dicha clave privada.

Son necesarios 3 operadores de DOCUMENTA S. A., de un total de 5, para activar y usar la clave privada de la dicha CA.

### 6.2.3. Custodia de la clave privada

La clave privada de la CA de DOCUMENTA S. A. se encuentra alojadas en dispositivos de hardware criptográfico con certificación FIPS-2 de nivel 3.

DOCUMENTA S. A. no almacena ni copia las claves privadas de sus suscriptores, ni de los módulos hardware que los contienen.

### 6.2.4. Copia de seguridad de la clave privada

La clave privada de la CA de DOCUMENTA S. A. está archivada bajo la protección de dispositivos seguros y a los que sólo las personal con rol de confianza autorizada por DOCUMENTA S. A. tiene acceso.

Los respaldos de clave privada de la CA de DOCUMENTA S. A. son únicamente para propósitos de recuperación en caso de una contingencia o desastre.

La clave privada de certificado persona física para firma digital del suscriptor no es respaldada por ningún motivo

en la CA de DOCUMENTA S. A., y éstas permanecen dentro de los límites de los dispositivos criptográficos donde fue generada.

### 6.2.5. Archivado de la clave privada

Las claves privadas nunca serán archivadas para garantizar el no repudio.

### 6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

La transferencia de la clave privada de la CA de sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de personal con rol de confianza autorizado por DOCUMENTA S. A.

### 6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en el módulo criptográfico FIPS 140-2 nivel 3 en el momento de la creación que hacen uso de dichos módulos y se guardan cifradas.

### 6.2.8. Método de activación de la clave privada

La clave privada tanto de la CA de DOCUMENTA S. A., se activa mediante la inicialización del software de CA por medio de la combinación mínima de operadores de la CA correspondiente. Éste es el único método de activación de dicha clave privada.

Concretamente, son necesarios 2 operadores de DOCUMENTA S. A. para activar la clave privada de cualquiera de la CA.

### 6.2.9. Método de desactivación de la clave privada

El Administrador de Sistemas designado por DOCUMENTA S. A. puede proceder a la desactivación de la clave de la Autoridad de Certificación de DOCUMENTA S. A. mediante la parada de la aplicación informática de la CA.

### 6.2.10. Método de destrucción de la clave privada

El procedimiento para la destrucción de las claves privadas de DOCMENTA S. A. requiere de una autorización para destruirlas.

La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del Módulo criptográfico de hardware la parte en la que estaban grabadas las claves, para ello, éste debe ser limpiado por medio de inicialización de ceros (zeroize command).

El procedimiento de destrucción de clave privada, debe estar documentado y realizado por personal con rol de confianza con control multipersona. La destrucción de la clave privada debe constar en los registros de auditoría.

#### 6.2.11. Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 nivel 3.

### 6.3. Otros aspectos de la gestión del par de claves

#### 6.3.1. Archivo de la clave pública

DOCUMENTA S. A mantiene un archivo de todos los certificados, los cuales incluyen las claves públicas, emitidos por un periodo de, al menos, diez (10) años. El control de dicho registro está a cargo del jefe de Área la CA de DOCUMENTA S. A.

El archivo dispone de medios de protección frente a las manipulaciones que pretendan efectuarse sobre la información contenida.

#### 6.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves

Los periodos de uso de la clave son descriptos en la sección 5.6 de la presente CPS.

### 6.4. Datos de activación

#### 6.4.1. Generación e instalación de los datos de activación

La CA de DOCUMENTA S. A. mantiene estrictos controles en los datos de activación para operar los módulos criptográficos.

Para ello cuenta con datos de activación de múltiples factores para protección de los accesos al uso de claves privadas.

Su activación requiere de un control de múltiples partes (es decir,“m” de “n”) con un valor mínimo de tres para “m”.

La CA de DOCUMENTA S. A. facilita a su suscriptor un dispositivo seguro de creación de firma, este dispositivo tiene la capacidad de generar datos de activación sin intervención de terceros.

#### 6.4.2. Protección de los datos de activación

Sólo el personal autorizado de la CA de DOCUMENTA S. A., posee las tarjetas criptográficas con capacidad de activación de la CA y conoce los PIN y contraseñas para acceder a los datos de activación.

El método desarrollado por DOCUMENTA S. A. permite a su suscriptor generar por sí solo, y sin intervención de terceros los datos de activación. El suscriptor es responsable de custodiar debidamente los datos de activación.

### 6.4.3. Otros aspectos de los datos de activación

Los datos de activación de los módulos criptográficos de la CA de DOCUMENTA S. A. son cambiados al menos una vez cada seis meses.

## 6.5. Controles de seguridad informática

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

### 6.5.1. Requerimientos técnicos específicos de seguridad informática

No está permitida la identificación única y general a los sistemas de la CA de DOCUMENTA CA. Cada proceso requiere una identificación exclusiva, y se sigue un sistema de autenticación jerárquico, Además se dispone de un método de desactivación automática en caso de inactividad, que requiere una re-autenticación.

DOCUMENTA S. A. cuenta con una política de seguridad que permite una administración efectiva del nivel de acceso de los usuarios para mantener la seguridad del sistema.

El personal de DOCUMENTA S. A. es identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.

El personal de DOCUMENTA S. A será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.

Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento que queden accesible a usuarios no autorizados.

Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos.

El acceso al repositorio público de DOCUMENTA S. A. deberá contar con control de accesos para modificaciones o borrado de datos.

Las actualizaciones y parches de los sistemas operativos deberían ser aplicados de manera oportuna y la utilización

de programas utilitarios del sistema debería ser restringida al personal autorizado, y debe estar estrictamente controlado.

### 6.5.2. Evaluación de la seguridad informática

DOCUMENTA S. A. evalúa de forma permanente su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así con la realización continua de controles de seguridad.

## 6.6. Controles de seguridad del ciclo de vida

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

### 6.6.1. Controles de desarrollo de sistemas

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de PKI de DOCUMENTA S. A.

La CA debe mantener controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la CA.

Los nuevos sistemas o para la expansión de los sistemas existentes, deben especificar los requisitos de control, seguir procedimientos de prueba de software y control de cambios para la implementación de software. Toda la documentación del ciclo de vida del sistema, debe estar disponible para su verificación.

La CA debe mantener controles sobre el acceso a las bibliotecas fuente de programas.

### 6.6.2. Controles de gestión de seguridad

DOCUMENTA S. A mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica y se realiza un seguimiento de las necesidades de capacidad.

### 6.6.3. Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas con algún impacto en la seguridad de la PKI.

DOCUMENTA S. A. realiza controles para proporcionar seguridad al dispositivo que realiza la generación de las claves. Para evitar posibles incidencias en los sistemas se establecen los siguientes controles:

- El hardware de generación de claves es probado antes de su puesta en producción.
- La generación de claves se producen dentro de los módulos criptográficos que cumplan los requisitos de la técnica y del negocio.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de la ceremonia de generación de claves.

## 6.7. Controles de seguridad de la red

El acceso a las diferentes redes de DOCUMENTA C. A. está limitado a personal debidamente autorizado. En particular:

- Se implementa controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos están configurados de forma que se impiden accesos y protocolos que no sean necesarios para las operaciones de servicio.
- Los datos sensibles son cifrados cuando se intercambian a través de redes no seguras.
- Se garantiza que los componentes locales de red están ubicados en entornos seguros, así como auditoria periódicas de sus configuraciones.

## 6.8. Sellado de tiempo

Sin estipulaciones.

# 7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

## 7.1. Perfil de certificado

El certificado digital cumple con:

- ITU-T X.509 V.3 Information technology Open systems interconnection TheDirectory: Public-key and attribute certificate frameworks
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. • ETSI TS 101 862 V.1.3.3 Qualified Certificates Profile
- RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile
- ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países". • RFC – 3279 '' Internet X.509 Public Key Infrastructure Algorithm Identifier'

**El certificado digital de CA de DOCUMENTA S. A. y los emitidos por el cumplen el siguiente formato:**

| PRINCIPAL | |
|---|---|
| **Campo x509v3** | **Descripción** |
| **Versión (Version)** | X.509 versión 3 (V3). |
| **SerialNumber** | Valor único emitido dentro del ámbito de una CA. |
| **Algoritmo de firma (Signature algorithm)** | Como mínimo SHA 256 RSA. |
| **Emisor (Issuer DN)** | Nombre de la CA que emite el certificado. Ver sección 7.1.4. |
| **Válido desde (Valid from)** | Este Campo especifica la fecha y hora a partir de la cual el certificado es válido. |
| **Válido hasta (Valid to)** | Este Campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. |
| **Sujeto (Suscriber DN)** | Nombre del suscriptor. Ver sección 7.1.4. |
| **Clave pública del sujeto (Subject Public Key)** | Codificado de acuerdo con el RFC 5280. Con un largo de clave mínima de 2048 bits y algoritmo RSA. |
| | |
| **Campo x509v3** | |

| | |
|---|---|
| **Identificador de clave de la entidad emisora (Authority Key Identifier)** | Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de confianza. Referencia el campo "Subject Key Identifier" de la CA. |
| **Identificador de la clave del titular (Subject Key Identifier)** | Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública. |
| **Política del certificado (Certificate Policies)** | Describe las políticas aplicables al certificado y la dirección URL donde se encuentra disponible la CP y CPS respectiva. |
| **Uso de la clave (Key usage)** | Indica los usos permitidos de la clave. Este campo debe ser marcado como un CAMPO CRÍTICO. Ver sección 1.4.1 Usos apropiados del certificado. |
| **Punto de distribución del CRL (Distribuition Points)** | Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. |
| **Acceso a la información de la autoridad (Authority Information Access)** | Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado de la CA. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. |
| **Usos extendidos de la clave** | Referencia otros propósitos de la clave, adicionales al uso. Solamente en el caso de certificado de persona física o jurídica este campo se especifica. |
| **Restricciones básicas (Basic Contraitns)** | Establecen las restricciones básicas. |
| **Huella Digital (Thumbprint)** | Resultado de aplicar algoritmos matemáticos a la información |
| **QcStatements** | Conforme al ETSI- TS 101 862 V.1.3.3. |

### 7.1.1. Número de versión

La PKI de DOCUMENTA S. A. soporta y utiliza certificados X.509 versión 3 (X.509 v3)

### 7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- KeyUsage. **Calificada como crítica.**
- CertificatePolicies. **Calificada como crítica.**
- SubjectAlternativeName. Calificada como no crítica.
- BasicConstraints. **Calificada como crítica.**
- Uso extendido de la clave. Calificada como no crítica.
- CRLDistributionPoint. Calificada como no crítica.
- Authority Key Identifier. Calificada como no crítica.
- Subject Key Identifier. Calificada como no crítica.
- QcStatements Calificada como no crítica

Las Políticas de Certificación de DOCUMENTA S. A. pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

La estructura del certificado, referente a la extensión **subject** del certificado, es la que se describe como ejemplo en la siguiente tabla:

| CAMPO | VALOR DE EJEMPLO |
|---|---|
| CN | CA-DOCUMENTA S. A. |
| O | DOCUMENTA S. A. |
| C | PY |
| SERIAL NUMBER | RUC 80050172-1 |

A continuación se detalla el contenido de las extensiones más importantes del **Certificado de la CA de DOCUMENTA S. A.**:

| CAMPO | COMPONENTE PROPUESTO | CRITICA |
|---|---|---|
| **1. Versión** | V3 | |
| **2. Signature Algorithm** | sha256WithRSAEncryption | |
| **3. Issuer** | CN = AUTORIDAD CERTIFICADORA RAÍZ DEL PARAGUAY<br>O = MINISTERIO DE INDUSTRIA Y COMERCIO<br>C = PY | |
| **4. Validez** | [10 AÑOS] | |
| **5. Subject** | CN = CA-DOCUMENTA S.A.<br>O = DOCUMENTA S. A.<br>C = PY<br>SERIALNUMBER = RUC 80050172-1 | |
| **6. Subject Public Key Info** | Algoritmo: RSA Encryption<br>Longitud:4096 bits | |
| **7. Certificate Policies**<br>**.Policy Identifier**<br>**.URL CPS**<br>**.Notice Referente** | **Se utilizará**<br>Directivas del certificado<br>http://www.acraiz.gov.py/cps/politicas.pdf<br>Certificado emitido dentro del marco de la Infraestructura de Claves Públicas del Paraguay bajo la jerarquía de su Autoridad Certificadora Raíz. | **SI** |
| **8. CRLDistributionPoints** | http://www.acraiz.gov.py/arl/ac_raiz_py.crl | NO |
| **9. Auth. Information Access**<br>**.CAIssuers**<br>**.OCSP** | **Se utilizará**<br>http://www.acraiz.gov.py/crt/ac_raiz_py_sha256.crt<br>http://www.documenta.py/firmadigital/oscp | NO |
| **10. BasicConstraints** | Tipo de asunto=Entidad de certificación (CA)<br>Restricción de longitud de ruta=0 | **SI** |

| | | |
|---|---|---|
| **11. KeyUsage** | **Firma de Certificado (Certificate Signing)**<br><br>**Firma de CRL (CRL Signing).** | **SI** |
| **12. Subject Key Identifier** | **SHA-1 hash de la clave pública** | NO |
| **14. Authority Key Identifier**<br><br>**.KeyIdentifier**<br><br>**.AuthorityCertIssuer**<br><br>**.AuthorityCertSerialNumber** | **Se utilizará**<br><br>**SHA-1 hash de la clave pública del emisor**<br><br>**No utilizado**<br><br>**No utilizado** | NO |

### 7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de objeto (OID) de algoritmo criptográfico

- sha256WithRSAEncryption (1.2.840.113549.1.1.11).

Identificador de objeto (OID) de clave pública

- RSAEncryption (1.2.840.113549.1.1.1).

### 7.1.4. Formatos de nombres

Los certificados emitidos por la CA de DOCUMENTA S. A. contienen el DistinguishedName X.500 del emisor y del titular del certificado en los campos IssuerName y SubjectName respectivamente.

### 7.1.5. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a DistinguishedNames X.500, que son únicos y no ambiguos.

Los nombres se escriben en mayúsculas y sin tildes, únicamente se debe aceptar el carácter ‘’Ñ ‘’como un caso especial para los nombres de personas físicas y jurídicas.

El código de país es de dos caracteres y se asigna de acuerdo al estándar ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”.

### 7.1.6. Identificador de objeto (OID) de la Política de Certificación a definir en cada Política de Certificación.

No estipulado.

### 7.1.7. Uso de la extensión “PolicyConstraints”

No estipulado.

### 7.1.8. Sintaxis y semántica de los "PolicyQualifier"

La extensión Certificate Policies contiene los siguientes Policy Qualifiers:

- URL CPS: contiene la URL, la CPS y la CP que rigen el certificado.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

En el campo NoticeReference se incluirá un texto con información básica sobre el certificado y las políticas a que está sujeto.

### 7.1.9. Semántica de procesamiento para la extensión de Políticas de Certificado (Certificate Policies)

No estipulado.

## 7.2. Perfil de CRL

Las listas de revocación de certificados cumplen con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" y contienen los elementos básicos especificados en el siguiente cuadro:

| Campo | Valor o restricciones |
|---|---|
| **Versión (Version)** | X.509 versión 2 (v2). |
| **Algoritmo de firma (Signature Algorithm)** | Algoritmo usado para la firma del CRL. Como mínimo es SHA256With RSAEncryption |
| **Emisor (Issuer)** | Entidad que emite y firma la CRL. |
| **Fecha efectiva (Effective Date)** | Fecha de emisión de la CRL. |
| **Siguiente actualización (NextUpdate)** | Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL está acorde con lo requerido en la sección 4.9.7 |
| **Certificados revocados (Certificate Revoked)** | Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación. |
| **Extensiones** | |
| **Número CRL(CRL Number)** | **Orden secuencial de emisión de CRL** |

| | |
|---|---|
| **Identificador de clave de Autoridad (Authority Key Identifier)** | Identificador de la clave pública de CA que emite. |
| **Punto de distribución del CRL (Distribuition Points)** | Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado |

### 7.2.1. Número de versión

La PKI de DOCUMENTA S. A. soporta y utiliza CRL X.509 versión 2 (v2).

### 7.2.2. CRL y extensiones

- Número CRL (CRL Number).Calificada como crítica.
- Identificador de clave de Autoridad. Calificada no como crítica.
- Puntos de distribución de las CRL. Calificada no como crítica.

## 7.3. Perfil de OCSP

### 7.3.1. Número(s) de versión

El perfil es el definido en la RFC 2560. “X.509 nternet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

### 7.3.2. Extensiones OCSP

No estipulado.

# 8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

## 8.1. Frecuencia o circunstancias de los controles para cada Autoridad

Se llevará a cabo una auditoría externa por el MIC o entidad que ellos habiliten para el efecto sobre la PKI de DOCUMENTA S. A. de forma regular al menos una vez al año. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta CPS y las CP.

DOCUMENTA S. A. realizará una auditoría interna al menos una vez al año.

## 8.2. Identificación/cualificación del auditor

Todo equipo o persona designada para realizar una auditoría de seguridad sobre la PKI de DOCUMENTA S. A. deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la CA de DOCUMENTA S. A.

## 8.3. Relación entre el auditor y la Autoridad auditada

Al margen de la función de auditoría, el auditor externo y la parte auditada (DOCUMENTA S. A.) no deberán tener relación alguna que pueda derivar en un conflicto de intereses.

Para el caso de las Auditorías internas, el Auditor debe ser independiente funcionalmente del área objeto de evaluación.

## 8.4. Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios de la CA DE DOCUMENTA S. A. con esta CPS y las CP aplicables. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

El ámbito de actividad de una auditoría incluirá, al menos a:

- Política de seguridad.
- Controles de seguridad física y estándares técnicos de seguridad.
- Evaluación tecnológica:
  - Confidencialidad y calidad de los sistemas de control.
  - Integridad y disponibilidad de los datos.
  - Cumplimiento de los estándares tecnológicos.

- Administración de los servicios de la CA .

- Selección y seguridad del personal
- Cumplimiento de la Política y Declaración de Prácticas de Certificación.
- Contratos.
- Cumplimiento de la legislación vigente, entre otros.

## 8.5. Acciones a tomar como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría (interna o externa) dará lugar a la adopción de medidas correctivas. El auditor, será el responsable de la determinación de las mismas.

En caso de detectarse una irregularidad en la Auditoría externa realizada a la CA de DOCUMENTA S. A., podrán tomarse entre otras las siguientes acciones dependiendo de la gravedad de la misma:

- Indicar las irregularidades, pero permitir al PSC que continúe sus operaciones hasta la próxima Auditoría programada
- Permitir al PSC que continúe sus operaciones con un máximo de treinta días corridos, tiempo durante el cual deberá subsanar la irregularidad detectada, caso contrario se procederá a la Suspensión.
- Suspender la operación del PSC.

En caso que se ordene la suspensión de actividades del PSC, solo podrá realizar servicios de soporte técnico y atención a los suscriptores ya existentes, en ningún caso podrá seguir brindando servicios de certificación.

## 8.6. Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría a la DGFDyCE del MIC, al Coordinador de Seguridad de DOCUMENTA S. A., así como a gerencia de DOCUMENTA S. A. y de la Autoridad en la que se detecten incidencias.

# 9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

## 9.1. Tarifas

### 9.1.1. Tarifas de emisión de certificado o renovación

Las tarifas de emisión y renovación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

### 9.1.2. Tarifas de acceso a los certificados

Las tarifas de acceso a los certificados se especifican en la Política de Certificación que les sea de aplicación.

### 9.1.3. Tarifas de acceso a la información de estado o revocación

Las tarifas de acceso a la información de estado o revocación de cada certificado se especifican en la Política de Certificación que le sea de aplicación.

### 9.1.4. Tarifas de otros servicios tales como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta CPS, ni las políticas de certificación administradas por la DOCUMENTA S. A., ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la elaboración del presente documento.

### 9.1.5. Política de reembolso

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte de la CA de DOCUMENTA S. A. para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente.

## 9.2. Responsabilidades económicas

DOCUMENTA S. A. dispone de la solvencia financiera necesaria para hacer frente a las responsabilidades que la legislación vigente le obliga a asumir. Dichas responsabilidades se encuentran cubiertas mediante póliza de responsabilidad civil, por el importe de 70 salarios mínimos.

Las Políticas de Certificación aplicables a cada tipo de certificado establecerán la cuantía máxima hasta la que se extenderá la responsabilidad por daños y perjuicios de DOCUMENTA S. A. frente a suscriptores y terceros de buena fe.

## 9.3. Confidencialidad de la información

Se establece el siguiente régimen de confidencialidad de los datos relativos a la CA de DOCUMENTA S. A.:

### 9.3.1. Ámbito de la información confidencial

Se declara expresamente como información confidencial y no podrá ser divulgada a terceros, excepto en los casos en que la normativa exija lo contrario:

- Las claves privadas de las Autoridad Certificadora de Documenta S. A.
- La información relativa a las operaciones que lleve a cabo de la CA DOCUMENTA S. A.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- Documentaciones que guardan relación con la Solicitud de suscriptores.
- Planes de contingencia y recuperación de desastres.
- Información o documentos que la CA Raíz haya determinado como confidencial.
- Registros de Auditoría.
- Los planes de negocio y estados financieros de los suscriptores.
- Se debe asegurar la reserva de toda información que mantiene la CA, que pudiera perjudicar la normal realización de las operaciones.

### 9.3.2. Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente Declaración de Prácticas de Certificación.
- La incluida en las Políticas de certificación que le sean de aplicación.
- Los certificados emitidos por la CA de DOCUMENTA S. A.
- La lista de los certificados revocados.

### 9.3.3. Deber de secreto profesional

Los empleados de DOCUMENTA S. A. y otras entidades externos a ellos que participen en cualesquiera tareas propias o derivadas de la PKI de DOCUMENTA S. A. están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable recogida fundamentalmente en el Reglamento Interno de DOCUMENTA S. A..

Asimismo el personal contratado que participe en cualquier actividad u operación de la PKI de DOCUMENTA S. A estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con DOCUMENTA S. A.

## 9.4. Protección de la información personal

DOCUMENTA S. A. está obligada a garantizar la protección, la confidencialidad y el debido uso de la información suministrada por los usuarios de los servicios de certificación de conformidad con normativa vigente.

### 9.4.1. Plan de Privacidad

La CA de DOCUMENTA S. A debe implementar políticas de privacidad de información, de acuerdo con la normativa vigente.

No se puede divulgar o vender información de los suscriptores o información de identificación de éstos.

### 9.4.2. Información tratada como privada

Cualquier información acerca de los suscriptores que no esté públicamente disponible a través del contenido del certificado emitido y servicios de CRL, debe ser tratada como información privada.

### 9.4.3. Información que no es considerada como privada

El tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa vigente al efecto. Únicamente se considera pública la información contenida en el certificado.

### 9.4.4. Responsabilidad para proteger información privada

La CA de DOCUMENTA S.A debe asegurar que la información privada no pueda ser comprometida o divulgada a terceras partes.

### 9.4.5. Notificación y consentimiento para usar información privada

La información privada no puede ser usada sin el consentimiento de las partes. Consentida, la CA de DOCUMENTA S. A. no requiere notificar a los suscriptores para usar información privada.

#### 9.4.6. Divulgación de acuerdo con un proceso judicial o administrativo

Para divulgar información privada se requiere de una orden judicial que así lo determine y se divulgará estrictamente la información solicitada.

#### 9.4.7. Otras circunstancias de divulgación de información

La información privada podrá ser divulgada en otras circunstancias, siempre que ésta resulte expresamente prevista por la legislación aplicable.

### 9.5. Derechos de propiedad intelectual

DOCUMENTA S. A. es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de DOCUMENTA S. A. sin la autorización expresa por su parte.

### 9.6. Representaciones y garantías

#### 9.6.1. Obligaciones de las CAs

La CA de DOCUMENTA S. A. es responsable del cumplimiento de sus obligaciones, según se establecen en esta CPS, incluso aunque parte de su actividad sea realizada mediante contratación externa. Asimismo, La CA de DOCUMENTA S. A. proporcionará sus servicios de forma consistente con esta CPS.

La CA de DOCUMENTA S. A. tiene las siguientes obligaciones:

- Realizar sus operaciones en conformidad con esta CPS.
- Proteger sus claves privadas.
- Emitir certificados en conformidad con las Políticas de Certificación que les sean de aplicación.
- Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 v3 y con los requerimientos de la solicitud.
- Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Publicar los certificados cuando sea necesario para interactuar con otros usuarios o sistemas informáticos que así lo requieran.

- Revocar los certificados en los términos de la sección 4.4 Revocación de Certificados y publicar los certificados revocados en la CRL en el servicio Web referidos en el apartado 2.1 Repositorio, con la frecuencia estipulada en el punto 4.9.7 Frecuencia de emisión de CRLs Publicar esta CPS y las CP aplicables en el sitio web referido en el apartado 2.1 Repositorio.
- Comunicar los cambios de esta CPS y de las CP de acuerdo con lo establecido en el apartado 9.10.2 Periodo y mecanismo de Notificación
- Garantizar la disponibilidad de las CRLs de acuerdo con las disposiciones de la sección 4.9.9 de la presente CPS.
- En el caso que la CA proceda a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con las Políticas de certificación que les sean de aplicación.
- Colaborar con las auditorías dirigidas por el MIC.
- Operar de acuerdo con la legislación aplicable.
- Proteger, en caso de haberlas, las claves bajo su custodia.
- No almacenar, ni copiar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados emitidos con el propósito de utilizarse para firma Digital.
- Mantener la confidencialidad de la información relativa a los titulares y suscriptores de certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido del titular o suscriptor del certificado original.
- Conservar registrada toda la información y documentación relativa a un certificado calificado durante diez años.

### 9.6.2. Obligaciones de las RAs

DOCUMENTA S. A. en su función de RA debe cumplir las siguientes obligaciones:

- Identificar correctamente al Titular y/o Solicitante y a la organización que represente, conforme a los procedimientos que se establecen en esta CPS y en las Políticas de Certificación específicas para cada tipo de certificado, utilizando cualquiera de los medios admitidos en derecho.

- Formalizar la expedición de Certificados con el Titular en los términos y condiciones que establezcan las Políticas de Certificación
- Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del certificado y en el proceso de revocación del mismo.
- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS.

### 9.6.3. Obligaciones de los titulares de los certificados

Es obligación de los titulares de los certificados emitidos bajo la presente CPS:

- Suministrar información exacta, completa y veraz con relación a los datos que los encargados de su verificación les soliciten para realizar el proceso de registro.
- Informar a los responsables de la CA de DOCUMENTA S. A. de cualquier modificación de esta información.
- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta CPS y en las CP que sean de aplicación, así como las modificaciones de las mismas.
- Limitar y adecuar el uso del certificado al ámbito estipulado por la Política de Certificación pertinente y la presente CPS.
- Poner el cuidado y medios necesarios para garantizar la custodia de su dispositivo criptográfico, evitando su pérdida, divulgación, modificación o uso no autorizado.
- El proceso de obtención de los certificados exige la elección personal de un PIN de control del dispositivo criptográfico y de activación de las claves privadas y un PUK de desbloqueo. Es responsabilidad del titular mantener bajo su exclusivo conocimiento el valor del PIN y el del PUK.
- Solicitar inmediatamente la revocación de un certificado en el caso de detección de inexactitudes en la información contenida en el mismo o tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por:

pérdida, robo, compromiso potencial, conocimiento por terceros del PIN y/o PUK.

- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación.
- No transferir ni delegar a un tercero sus responsabilidades sobre un certificado que le haya sido asignado.
- Cualquier otra que se derive de la ley, su reglamentación, de esta CPS o de las Políticas de Certificación.

### 9.6.4. Obligaciones de los terceros que confían o acepten los certificados

Es obligación de los terceros que aceptan y confían en los certificados emitidos por la CA de DOCUEMENTA S. A.:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de la recepción de los documentos firmados digitalmente mediante la comprobación de que el certificado es válido y no ha caducado o ha sido revocado.
- Asumir su responsabilidad en la verificación de las firmas digitales.

Asumir su responsabilidad en la comprobación de la validez y revocación de los certificados que acepta y en que confía.

Tener conocimiento de las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y aceptar sujetarse a las mismas.

Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

## 9.7. Exención de responsabilidades

La CA de DOCUMENTA S. A. solo responderá en el caso de incumplimiento de las obligaciones contenidas en Ley Nº 4017/2010, Ley Nº 4610/2014, decreto N° 7369/2011, en la presente CPS y en las Políticas de Certificación específicas.

La CA de DOCUMENTA S. A. sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación

asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

La CA de DOCUMENTA S. A. no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

La CA de DOCUMENTA S. A. no asume ninguna responsabilidad en caso de cualquier tipo de pérdida o perjuicio:

- De los servicios que presta, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta CPS.
- Ocasionados por el mal uso de la información contenida en el certificado.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la CA de DOCUMENTA S. A.
- DOCUMENTA S. A. no asumirá responsabilidad alguna en relación al uso de los Certificados emitidos por su CA y el par de claves privada/pública asociado a sus titulares para cualquier actividad no especificada en la CPS o en las Políticas de Certificación correspondientes. +
- DOCUMENTA S. A., como Prestador de Servicios de Certificación, no será responsable del contenido de los documentos electrónicos, ni mensajes de datos firmados con sus certificados ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado o comunicaciones.

## 9.8. Limitaciones de las responsabilidades

A excepción de lo establecido por las disposiciones de la presente CPS, en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario Nº 7369/2011, La CA de DOCUMENTA S. A. no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían.

## 9.9. Indemnizaciones

La CA de DOCUMENTA S. A. responderá ante el tribunal contencioso administrativo correspondiente por los daños y perjuicios que se cause al firmante, terceros o a cualquier persona, en el ejercicio de su actividad como prestador de servicios de certificación en los términos establecidos en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011 y la presente CPS. A tal efecto para el cálculo del monto de la indemnización se aplicarán las normas generales del procedimiento administrativo y responsabilidad contractual o extracontractual correspondientes.

### 9.9.1. Indemnizaciones por daños ocasionados por la CA de DOCUMENTA S. A.

Las indemnizaciones que tenga que asumir la CA de DOCUMENTA S. A. por daños efectuados a terceros se hará en base a los términos establecidos en la establecidos en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011 y la presente CPS.. La CA de DOCUMENTA S. A. no asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían o acepten los certificados.

### 9.9.2. Indemnizaciones por los daños ocasionados por los Suscriptores

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado digital durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones por responsabilidad civil y penal según lo determinen los tribunales correspondientes de conformidad con Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011.

### 9.9.3. Indemnizaciones por los daños ocasionados por los Terceros que confían

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado digital durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones por responsabilidad civil y penal según lo determinen Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario N° 7369/2011.

## 9.10. Período de validez

### 9.10.1. Plazo

Esta CPS entra en vigor desde el momento de su publicación en el repositorio de CA de DOCUMENTA S. A. previa aprobación por el MIC.

Esta CPS estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión.

### 9.10.2. Sustitución y derogación de la CPS

Esta CPS será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la CPS quede derogada se retirará del repositorio público de la CA de DOCUMENTA S. A., si bien se conservará durante 10 años.

### 9.10.3. Efectos de la finalización

Las obligaciones y restricciones que establece esta CPS, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de la CA de DOCUMENTA S. A. , nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

## 9.11. Notificaciones individuales y comunicaciones con los participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta CPS se realizará mediante mensaje electrónico o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 1.5 Administración de las Políticas. Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

## 9.12. Procedimientos de cambios en las especificaciones

### 9.12.1. Procedimiento para los cambios

La Autoridad con atribuciones para revisar y aprobar cambios sobre la CPS y las PCs de la CA de DOCUMENTA S. A. es la Dirección General de Firma Digital y Comercio Electrónico del MIC.

### 9.12.2. Circunstancias en las que el OID debe ser cambiado

Sin estipulaciones.

## 9.13. Reclamaciones

Todas reclamaciones entre usuarios y la CA de DOCUMENTA S. A. deberán ser comunicadas por la parte en disputa a la CA de DOCUMENTA S. A., con el fin de intentar resolverlo entre las mismas partes.

En el caso de que no se llegue a un acuerdo entre las partes, la resolución de cualquier conflicto que pudiera surgir se someterá a los juzgados y tribunales de la ciudad capital del República del Paraguay.

## 9.14. Normativa aplicable

La CA de DOCUMENTA S. A. estará sujeta a las leyes de la República del Paraguay, en particular a la normativa que rige la materia.

## 9.15. Cumplimiento de la normativa aplicable

La presente CPS se adecua a legislación vigente aplicable a la materia.

## 9.16. Estipulaciones diversas

### 9.16.1. Cláusula de aceptación completa

Todos los Terceros que Confían asumen en su totalidad el contenido de la última versión de esta CPS y de las CP que sean de aplicación.

### 9.16.2. Asignación

Sin estipulaciones.

### 9.16.3. Independencia/divisibilidad

En el caso de que una o más cláusulas de esta CPS sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, el resto de las cláusulas de estas políticas se mantendrán vigentes.

### 9.16.4. Aplicación (Honorarios de Abogados y renuncia de derechos)

Sin estipulaciones.

### 9.16.5. Fuerza mayor

Los Acuerdos de Suscriptores incluyen cláusulas de fuerza mayor para proteger a la CA de DOCUMENTA S. A.

### 9.16.6. Resolución por la vía judicial

Los conflictos entre la CA de DOCUMENTA S. A. , suscriptores y terceros que surjan como Prestador de Servicios de Certificación se resolverán, una vez agotada la vía gubernativa, ante el tribunal Contencioso-Administrativo correspondiente.

## 9.17. Otras estipulaciones

El PSC habilitado de conformidad a los términos de una CP derogada de la CA Raiz, se adecuará a las disposiciones de la nueva CP en el plazo establecido por la Resolución que la ponga en vigencia.

La CPS Y CPs de la CA de DOCUMENTA S. A. guarda concordancia con las disposiciones establecidas por la Infraestructura de Claves Publicas del Paraguay.

# 10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP”.
- RFC 3647: “Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.
- ISO 3166 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- Ley Nro. 4017/2010 ‘’De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico’’.
- Ley Nro. 4610/2012 que modifica y amplía la Ley Nro. 4017/2010.
- Decreto Reglamentario Nro. 7369/2011.
- CP y CPS de la CA raíz del Paraguay.