CONTROL DOCUMENTAL

DOCUMENTO	
Título: Política de Certificación de Firma Digital Tipo F2 de la CA de Documenta S.A.	**Soporte lógico:** https://www.documenta.com.py/firmadigital/descargas
Fecha: 02/01/2017	**Ubicación física:** Documenta S.A.
Código: PKIpy-DocSA-CPF2v1.0.0	
Versión: 1.0.0	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
1.0.0	02/01/2017	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**
Javier Dávalos	Beltrán Ortiz	José Oricchio	José Minardi
Supervisor Firma Digital	Coordinador de Seguridad Documenta S.A.	Director ejecutivo Documenta S.A.	Presidente Documenta S.A.

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 Paraguay.

Este documento recoge la **POLITICA DE CERTIFICACION DE FIRMA DIGITAL TIPO F2 de la CA 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 Política de Certificación (CP por sus siglas en Ingles) 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.

Los certificados regulados por la presente CP sólo deben ser utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de identidad de sus informaciones para personas físicas o jurídicas.

Esta CP 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	Política de Certificación de Firma Digital Tipo F2 de la CA de DOCUMENTA S.A.
Versión del documento	1.0.0
Estado del documento	Versión inicial
Fecha de emisión	02/01/2017
Fecha de expiración	No aplicable
Ubicación de la CP	https://www.documenta.com.py/firmadigital/descargas/cpf2.pdf
CPS relacionada	Declaración de Prácticas de Certificación de la CA de DOCUMENTA S.A. V2.0

Las políticas de certificación incluidas en el presente documento son:

Nombre de la política	Política de Certificación de Firma Digital Tipo F2 Para Persona Física de la CA de DOCUMENTA S.A.
Tipo de certificados asociados	F2 Persona Física
Versión del documento	1.0.0
Estado del documento	Versión inicial
Fecha de emisión	02/01/2017
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.48315.1.1.1.6.1.1

Nombre de la política	Política de Certificación de Firma Digital Tipo F2 Para Persona Jurídica de la CA de DOCUMENTA S.A.
Tipo de certificados asociados	F2 Persona Jurídica
Versión del documento	1.0.0
Estado del documento	Versión inicial
Fecha de emisión	02/01/2017
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.48315.1.1.1.6.2.1

Nombre de la política	Política de Certificación de Firma Digital Tipo F2 Para Equipos o Aplicaciones de la CA de DOCUMENTA S.A.
Tipo de certificados asociados	F2 Equipo o Aplicaciones
Versión del documento	1.0.0
Estado del documento	Versión inicial
Fecha de emisión	02/01/2017

Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.48315.1.1.1.6.3.1

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. Prestadores de Servicio de Soporte (PSS).
4. Suscriptores.
5. Terceros que confían en los certificados de la PKI del Paraguay.
6. Otros Participantes.

1.3.1 Autoridades Certificadoras (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 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. Se constituye como CA Raíz del Paraguay el MIC.
- **Prestador de Servicios de Certificación (PSC):** es la persona jurídica que emite certificados digitales a los usuarios finales.

  El PSC DOCUMENTA S.A. una vez habilitado, pasó a ser parte de la cadena de confianza de la PKI Paraguay, y cuenta 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 CP y el acuerdo suscrito con la CA.

DOCUMENTA S.A. cumple funciones de RA. Además, podrá mediante un contrato de prestación de servicio establecer Autoridades de Registros Delegadas siempre y cuando las mismas se estén autorizadas por la CA Raíz, en todo el territorio de la república, cumpliendo las normas y procedimientos establecidos en el documento "Características Mínimas de Seguridad para las Autoridades de Registro de la Infraestructura de Claves Publicas del Paraguay" y la normativa vigente, previa comunicación y autorización de la AA. Siempre bajo el control y supervisión de DOCUMENTA S.A.

Los datos referentes a las RA habilitadas por DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.documenta.com.py/firmadigital/ra

La CA de DOCUMENTA S.A. mantiene publicada en el sitio las siguientes informaciones actualizadas:

- Identificación y vinculación de todas las RA habilitadas, con informaciones sobre las CP que implementan,
- Para cada RA habilitada, las direcciones de sus instalaciones técnicas, cuyo funcionamiento haya sido autorizado por la CA Raíz.
- Para cada RA habilitada, el tipo de vínculo con eventuales locales provisorios autorizados por la CA Raíz, con fecha de creación y cierre de actividades;
- Identificación y vínculo de las RA deshabilitadas dentro de la cadena PKI Paraguay, con su respectiva fecha de cese de actividades;
- Instalaciones técnicas de la RA habilitada que ha dejado de operar, con su respectiva fecha de cierre de actividades;
- Acuerdos operacionales celebrados entre las RA vinculadas con otra RA dentro de la PKI Paraguay, si fuera

el caso.

1.3.3 Prestadores de Servicios de Soporte (PSS)

PSS son entidades externas a las que recurre DOCUMENTA S.A. para desempeñar actividades descritas en esta CP o en la CPS y se clasifican en dos categorías, conforme al tipo de servicio prestado.

- Disponibilización de infraestructura física y lógica;
- Disponibilización de recursos humanos especializados;

Las informaciones actualizadas de las PSS habilitadas por DOCUMENTA S.A. se encuentran en la dirección de página web (URL) https://www.documenta.com.py/firmadigital/pss

1.3.4 Suscriptores

Se definen como aquellas personas físicas o jurídicas sujetos de derechos, con capacidad suficiente para 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 suscriptores toda persona física o jurídica a quien se emite un certificado digital, dentro de la jerarquía PKI Paraguay.

1.3.5 Parte que confía

En el ámbito de esta CP, las partes que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por DOCUMENTA S.A. dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.6 Otros Participantes

No estipulado

1.4. Uso del Certificado

1.4.1 Usos apropiados del Certificado

Los certificados regulados por la presente CP sólo deben ser utilizados en aplicaciones como confirmación de identidad y firma de documentos electrónicos con verificación de identidad de sus informaciones (tipos F). Para determinar si es posible utilizar un certificado de firma digital del tipo F2 es necesario comprobar el valor de la extensión **'Key Usage'** del certificado en cuestión. Este campo deberá contener los siguientes datos:

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

1.4.2 Usos prohibidos del certificado

Los certificados de firma digital tipo F2 no deben emplearse para actividades especificadas como prohibidas en la normativa vigente, la CPS o en esta CP.

1.5. Administración de la Política

1.5.1. Organización que administra el documento

Nombre	**DOCUMENTA S.A.**
Dirección	**Avda. General Máximo Santos N°698 Asunción – Paraguay**
Código Postal	**1535**
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	**1535**
Teléfono	**+59521492503/3**
Correo electrónico	firmadigital@documenta.com.py

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

Como establezca la CPS de DOCUMENTA S.A.

1.5.4. Procedimientos de aprobación de la CP

El MIC aprobará el contenido de la Política de Certificación de Firma Digital Tipo F2 de la CA 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.

Agente de Registro: Persona responsable de la ejecución de actividades relacionadas con la RA, que realiza la validación y verificación de la solicitud de certificado.

Armario ignífugo: Armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.

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 Certificación Intermedia (CAI): Entidad cuyo certificado de clave pública ha sido firmado digitalmente por la autoridad de certificación raíz; es responsable de la emisión de certificados a usuarios finales.

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.

Autoridad de Validación (VA): Entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación. La VA, no necesita ser un organismo separado, sino que puede ser parte de la CA.

Cadena de certificación: Lista ordenada de certificados que contiene un certificado de usuario final y certificados de CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado de CA y a su vez, el emisor del certificado de CA es el titular del certificado de CA Raíz. El usuario final o la parte que confía, debe verificar la validez de los certificados en la cadena.

Ceremonia de claves: Procedimiento mediante el cual es generado un par de claves de CA, su clave privada es generada y almacenada en un módulo criptográfico, y debe ser respaldada con el mismo nivel de seguridad que la clave original. Este procedimiento debe ser documentado.

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: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que solo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.

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 pública y privada: La criptografía en la que se basa la PKI Paraguay, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado digital, mientras que a la otra se le denomina privada y está bajo la custodia del titular del certificado.

Cofre de seguridad: Compartimiento para almacenar materiales o documentos sensibles de la CA, debe ser resistente al fuego y ofrecer protección a aperturas forzadas.

Compromiso: Violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.

Data Center (Centro de Datos): Infraestructura compuesta por el espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una CA, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados digitales emitidos por la CA.

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 de los Certificados, cuyo proceso, es una función de la CA.

Emisor del certificado: Organización cuyo nombre aparece en el

campo emisor de un certificado.

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.

Grupo Electrógeno: Máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la CA, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.

Habilitación: Autorización que otorga el MIC al PSC para emitir certificados digitales a usuarios finales, una vez cumplidos los requisitos y condiciones establecidos en la norma.

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 documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Jerarquía PKI: Jerarquía de confianza que se conforma por un conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior (CA Raíz) garantiza la confiabilidad de una o varias de nivel inferior (PSC) y a su vez, de los certificados emitidos por éstos a los suscriptores.

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 almacenas 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#1: Estándar de criptografía de clave pública #1, desarrollado por RSA Security Inc., que proporciona las definiciones básicas y recomendaciones para la implementación de algoritmo RSA para criptografía de clave pública.

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 diferente del

titular, que decide aceptar y confiar en un certificado emitido bajo la jerarquía de 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 del Paraguay 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.

Solicitante de Certificado: Persona física o jurídica que solicita la emisión de un certificado a una CA.

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.

X. 509: Estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2 Acrónimos

C: País (del inglés, Country).

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

CAI: Autoridad de Certificación Intermedia (CAI por sus siglas en inglés Certificate Authority Intermediate.

CA Raíz: Autoridad Certificadora Raíz del Paraguay

CI: Cédula de identidad

CN: Nombre común (del inglés, Common Name).

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

certificate 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.

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).

HSM: Modulo de seguridad basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module).

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

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

MIC: Ministerio de Industria y Comercio.

O: Organización (del inglés Organization).

OCSP: Servicio de validación de certificados en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol).

OID: Identificador de Objeto (OID por sus siglas en inglés Object Identifier).

OU: Unidad Organizacional (OU, por sus siglas en inglés Organization Unit).

PIN: Número de Identificación Personal (por sus siglas en inglés, Personal Identification Number).

PKCS: Norma de criptografía de clave pública (PKCS por sus siglas en inglés, Public Key Cryptography Standards).

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).

RSA: Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman.

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).

TLS: Conexión de capa segura (TLS por sus siglas en inglés, Transport Layer Security)

UPS: Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, Uninterruptible Power Supply)

URL: Localizador uniforme de recursos (URL por sus siglas en inglés Uniform Resource Locator).

VA: Autoridad de Validación (VA por sus siglas en inglés Validation Authority).

2. RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

2.1 Repositorios

Como establezca la CPS de DOCUMENTA S.A.

2.2 Publicación de Información de Certificación

Como establezca la CPS de DOCUMENTA S.A.

2.3 Tiempo o frecuencia de Publicación

Como establezca la CPS de DOCUMENTA S.A.

2.4 Controles de Acceso

Como establezca la CPS de DOCUMENTA S.A.

3. Identificación y Autenticación

3.1 Nombres

Como establezca la CPS de DOCUMENTA S.A.

3.1.1 Tipos de Nombres

Como establezca la CPS de DOCUMENTA S.A.

3.1.2 Necesidad de Nombres significativos

Como establezca la CPS de DOCUMENTA S.A.

3.1.3 Anonimato o seudónimos de los suscriptores

Como establezca la CPS de DOCUMENTA S.A.

3.1.4 Reglas para interpretación de varias formas de Nombres

Como establezca la CPS de DOCUMENTA S.A.

3.1.5 Unicidad de nombres

Como establezca la CPS de DOCUMENTA S.A.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

Como establezca la CPS de DOCUMENTA S.A.

3.2 Validación inicial de identidad

3.2.1 Método para probar posesión de la Clave Privada

Como establezca la CPS de DOCUMENTA S.A.

3.2.2 Autenticación de identidad de Persona Jurídica

Como establezca la CPS de DOCUMENTA S.A.

3.2.3 Autenticación de identidad de persona física

Como establezca la CPS de DOCUMENTA S.A.

3.2.4 Autenticación de identidad de una máquina o aplicación

Como establezca la CPS de DOCUMENTA S.A.

3.2.5 Información del Suscriptor no verificada.

No estipulado.

3.2.6 Validación de la Autoridad (CAPACIDAD DE HECHO)

Como establezca la CPS de DOCUMENTA S.A.

3.2.7 Criterios para interoperabilidad

Como establezca la CPS de la CA de DOCUMENTA S.A.

3.3 Identificación y autenticación para solicitudes de re emisión de claves

3.3.1 Identificación y Autenticación para re emisión de claves

Como establezca la CPS de la CA de DOCUMENTA S.A.

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

Como establezca la CPS de la CA de DOCUMENTA S.A.

3.4 Identificación y autenticación para Solicitudes de Revocación.

Como establezca la CPS de la CA de DOCUMENTA S.A.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud del certificado

4.1.1 Quién puede presentar una solicitud de certificado

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.1.2 Proceso de Inscripción y responsabilidades

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.2 Procesamiento de la Solicitud del Certificado

4.2.1 Ejecución de las funciones de identificación y autenticación

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.2.2 Aprobación o rechazo de solicitudes de certificado

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.2.3 Tiempo para procesar solicitudes de Certificado

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.3 Emisión del certificado

4.3.1 Acciones de la CA durante la emisión de los certificados

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.3.2 Notificación al suscriptor sobre la emisión del Certificado Digital

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.4 Aceptación del certificado

4.4.1 Conducta Constitutiva de Aceptación de Certificado

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.4.2 Publicación del certificado por la CA

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.4.3 Notificación de la emisión del certificado por la CA a otras Entidades

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.5 Uso del par de Claves y del Certificado

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.5.1 Uso de la clave privada y del certificado por el Suscriptor

Como establezca la CPS de la CA de DOCUMENTA S.A.

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

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.6 Renovación del Certificado

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.6.1 Circunstancias para renovación de certificado

No estipulado.

4.6.2 Quién puede solicitar la renovación

No estipulado.

4.6.3 Procesamiento de Solicitudes de Renovación de Certificado

No estipulado.

4.6.4 Notificación al Suscriptor sobre la emisión de un nuevo certificado

No estipulado.

4.6.5 Conducta constitutiva de aceptación de un certificado renovado

No estipulado.

4.6.6 Publicación por la CA del Certificado Renovado

No estipulado.

4.6.7 Notificación por la CA de la emisión de un Certificado a otras entidades

No estipulado.

4.7 Re-emisión de claves de Certificado

La renovación con cambio de claves no está permitida por esta

CP, cuando un certificado requiera ser re-emitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de este CP.

4.7.1 Circunstancias para re-emisión de claves de certificado

No estipulado.

4.7.2 Quién puede solicitar la certificación de una clave publica

No estipulado.

4.7.3 Procesamiento de Solicitudes de re-emisión de claves de certificado

No estipulado.

4.7.4 Notificación al Suscriptor sobre la re-emisión de un nuevo certificado

No estipulado.

4.7.5 Conducta constitutiva de aceptación de un certificado re-emitido

No estipulado.

4.7.6 Publicación por la CA de los certificados re-emitidos

No estipulado.

4.7.7 Notificación por la CA de la re-emisión de un certificado a otras entidades

No estipulado.

4.8 Modificación de certificados

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 CP.

4.8.1 Circunstancias para modificación del certificado

No estipulado.

4.8.2 Quién puede solicitar modificación del certificado

No estipulado.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No estipulado.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

No estipulado.

4.8.5 Conducta constitutiva de aceptación del certificado modificado

No estipulado.

4.8.6 Publicación por la CA de los certificados modificados

No estipulado.

4.8.7 Notificación por la CA de emisión de certificado a otras entidades

No estipulado.

4.9 Revocación y suspensión

4.9.1 Circunstancias para la revocación

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.2 Quién puede solicitar revocación

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.3 Procedimiento para la solicitud de revocación

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.4 Periodo de gracia para solicitud de revocación

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.6 Requerimientos de verificación de revocación para las partes que confían

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.7 Frecuencia de emisión del CRL

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.8 Latencia Máxima para CRL

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.9 Requisitos de verificación de CRL

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.10 Disponibilidad de verificación de revocación/estado en línea

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.11 Requerimientos para verificar la revocación en línea

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.12 Otras formas de advertencias de revocación disponibles

No estipulado.

4.9.13 Requerimientos especiales por compromiso de clave privada

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.9.14 Circunstancias para suspensión

No estipulado.

4.9.15 Quién puede solicitar la suspensión

No estipulado.

4.9.16 Procedimiento para la solicitud de suspensión

No estipulado.

4.9.17 Límites del periodo de suspensión

No estipulado.

4.10 Servicios de comprobación de estado de certificado

4.10.1 Características operacionales

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.10.2 Disponibilidad del servicio

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.10.3 Características opcionales

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.11 Fin de la suscripción

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.12 Custodia y recuperación de claves

4.12.1 Política y prácticas de custodia y recuperación de claves

Como establezca la CPS de la CA de DOCUMENTA S.A.

4.12.2 Políticas y prácticas de recuperación y encapsulación de claves de sesión

No estipulado.

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

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.2 Acceso físico

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.3 Energía y Aire acondicionado

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.4 Exposiciones al Agua

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.5 Prevención y protección contra fuego

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.6 Almacenamiento de medios

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.7 Eliminación de residuos

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.1.8 Respaldo fuera de sitio

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.2.2 Número de personas requeridas por tarea

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.2.3 Identificación y autenticación para cada rol

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.2.4 Roles que requieren separación de funciones

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.3 Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y

autorización

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.3.2 Requerimientos y frecuencia de capacitación

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.3.3 Frecuencia y secuencia en la rotación de las funciones

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.3.4 Sanciones para acciones no autorizadas

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.3.5 Requisitos de contratación de terceros

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.3.6 Documentación suministrada al personal

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4 Procedimiento de registro de auditoría

5.4.1 Tipos de eventos registrados

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.2 Frecuencia de procesamiento del registro (LOGS)

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.3 Periodo de conservación del registro (LOGS) de auditoria

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.4 Protección del registro (LOGS) de auditoria

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.5 Procedimientos de respaldo (BACKUP) de registro (LOGS) de auditoria

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.6 Sistema de recolección de información de auditoría (interno vs externo)

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.7 Notificación al sujeto que causa el evento

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.4.8 Evaluación de vulnerabilidades

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.5 Archivos de registros

5.5.1 Tipo de registros archivados

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.5.2 Periodo de retención para archivos

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.5.3 Protección de archivos

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.5.4 Procedimientos de respaldo (BACKUP) de archivo

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.5.5 Requerimientos para sellado de tiempo de registros

Sin estipulaciones

5.5.6 Sistema de recolección de archivo (interno o externo)

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.5.7 Procedimientos para obtener y verificar información archivada

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.6 Cambio de clave

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.7 Recuperación de desastres y compromiso

5.7.1 Procedimiento para el manejo de incidente y compromiso

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.7.2 Corrupción de datos, software y/o recursos computacionales

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.7.3 Procedimientos de compromiso de clave privada de la entidad

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.7.4 Capacidad de continuidad del negocio después de un desastre

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.7.5 Actividades de las Autoridades de Registro

Como establezca la CPS de la CA de DOCUMENTA S.A.

5.8 Terminación de una CA

Como establezca la CPS de la CA de DOCUMENTA S.A.

6. CONTROLES TÉCNICOS DE SEGURIDAD

Los controles de seguridad técnica aplicables a los diferentes componentes de la PKI se encuentran descritos en la CPS de la CA de DOCUMENTA S.A. En este apartado únicamente se describen los controles de seguridad técnica particulares del tipo de certificados tratado.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Compete a la CA Raíz el seguimiento de la evolución tecnológica y en caso necesario, actualizar las normas y los algoritmos criptográficos utilizados en la PKI-Paraguay.

Cuando el titular del certificado es una persona física, éste será responsable de generar el par de claves criptográficas. Cuando el titular del certificado es una persona jurídica, su representante (s) legal (es), será la persona responsable de la generación de pares de claves criptográficas y del uso del certificado.

El algoritmo a ser utilizado para las claves criptográficas de titulares de certificados, está definido en el documento NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

Para ser generada, la clave privada de la persona física o jurídica titular del certificado deberá ser grabada y cifrada por un algoritmo simétrico aprobado en el documento NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY, en un medio de almacenamiento definido para cada tipo de certificado previsto por la Autoridad de Aplicación, conforme a lo estipulado en la siguiente tabla:

Tipo de Certificado	Medio de almacenamiento
F2	Hardware criptográfico homologado por la Autoridad de Aplicación

La clave privada debe transportarse encriptada, utilizando los mismos algoritmos citados en el párrafo anterior, entre el dispositivo generador y el medio utilizado para su

almacenamiento.

Los medios de almacenamiento de claves privadas, garantizarán, por medios técnicos y de procedimiento adecuados, como mínimo, que:

a) la clave privada es única y su confidencialidad es suficientemente asegurada;

b) la clave privada no puede, con seguridad razonable, ser deducida y debe estar protegida contra falsificaciones realizadas a través de la tecnología disponible en la actualidad; y

c) la clave privada puede ser eficazmente protegida por el legítimo titular contra su utilización por parte de terceros.

Esos medios de almacenamiento no deben modificar los datos que serán firmados ni debe impedir que esos datos sean presentados al firmante antes del proceso de firma.

6.1.2 Entrega de la clave privada al suscriptor

La clave privada de los certificados de firma digital tipo F2 es generada por el propio titular, por lo que en ningún caso será entregada al mismo.

6.1.3 Entrega de la clave pública al emisor del certificado

El titular del certificado, a través de un medio electrónico seguro, entrega su clave pública a la CA de DOCUMENTA S.A. o a su correspondiente RA vinculada en el formato definido en el documento NORMAS DE ALGORITMOS CRIPROGRÁFICOS DE LA PKI PARAGUAY

6.1.4 Entrega de la clave pública de la CA a las partes que confían

La clave pública de la CA de DOCUMENTA S.A. está a disposición de los terceros que confían en el Repositorio (ver apartado 2.1) en el formato establecido en el documento NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY

6.1.5 Tamaño de la clave

Los algoritmos y tamaños de clave a ser utilizados en los certificados de firma digital tipo F2 emitidos por la CA de DOCUMENTA S.A, se definen en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

6.1.6 Generación de parámetros de clave asimétricas y verificación de calidad

Los parámetros de generación de claves asimétricas de las entidades titulares de certificados, adoptará el estándar definido en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

Los parámetros de verificación de calidad, deberán ser verificados de acuerdo con las normas establecidas por el patrón definido en el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

6.1.7 Propósitos de usos de clave (CAMPO KEY USAGE X509 V3)

Los usos admitidos de la clave para los certificados de firma digital tipo F2 vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos.

El contenido de dichas extensiones para los de firma digital tipo F2 se puede consultar en el apartado 7.1 del presente documento.

6.1.8 Generación de clave por hardware o software

El proceso de generación de claves criptográficas, deberá ser realizado, para los certificados del tipo F2 en hardware.

6.2 Controles de ingeniería del módulo criptográfico y protección de la clave privada

6.2.1 Estándares y controles del módulo criptográfico

El estándar requerido para los módulos criptográficos con certificados del tipo F2, es el FIPS 140-1 o FIPS 140-2 o superior.

Los estándares requeridos para los módulos de generación de las claves criptográficas, son especificados en el documento NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

6.2.2 Control multi-persona de la clave privada

Las claves privadas de los certificados del tipo F2 no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el titular.

6.2.3 Custodia/recuperación de la clave privada

La custodia de las claves privadas de los certificados de firma digital (tipo F) la realizan los propios titulares de las mismas.

6.2.4 Respaldo/copia de la clave privada

En ningún caso se realizarán copias de seguridad de las claves privadas de firma digital para garantizar el no repudio.

6.2.5 Archivado de la clave privada

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

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

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

DOCUMENTA S.A. no podrá almacenar la clave privada del titular de certificados de firma digital.

6.2.8 Método de activación de la clave privada

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de al menos un factor de seguridad.

6.2.9 Métodos de desactivación de la clave privada

No estipulado.

6.2.10 Destrucción de la clave privada

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

6.2.11 Clasificación del módulo criptográfico

La capacidad del módulo criptográfico utilizado en los dispositivos se realiza conforme a lo que dicta el documento NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave publica

Las claves públicas de los titulares de los certificados de firma digital (tipo F), así como las CRL emitidas, serán almacenadas por la CA de DOCUMENTA S.A., después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

6.3.2 Periodo operacional del certificado y periodo de uso del par de claves

Las claves privadas de los certificados de firma digital deberán ser utilizadas por sus titulares únicamente durante el periodo de validez correspondiente.

Las correspondientes claves publicas podrán ser utilizadas durante

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

El periodo de validez de los certificados de firma digital de tipo F2 es como máximo de dos (2) años desde el momento de emisión del mismo.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Para certificados de firma digital tipo F2 la generación y almacenamiento del par de claves son realizados en dispositivos criptográficos hardware con capacidad de generación de claves siendo activados y protegidos por contraseñas y/o PIN.

6.4.2 Protección de los datos de activación

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.4.3 Otros aspectos de los datos de activación

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.5 Controles de seguridad del computador

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.5.2 Clasificación de la seguridad del computador

No estipulado.

6.5.3 Controles de seguridad para las autoridades de registro

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.6 Controles técnicos del ciclo de vida

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.6.1 Controles para el desarrollo del sistema

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.6.2 Controles de gestión de seguridad

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.6.3 Controles de seguridad del ciclo de vida

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.6.4 Controles en la generación de CRL

No estipulado.

6.7 Controles de seguridad de red

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.7.1 Directrices generales

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.7.2 Firewall

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.7.3 Sistema de Detección de Intruso (IDS)

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.7.4 Registro de acceso no autorizado a la red

Como establezca la CPS de la CA de DOCUMENTA S.A.

6.8 Controles de ingeniería del módulo criptográfico

Los módulos criptográficos utilizados para el almacenamiento de la clave privada del titular del certificado deben ser homologados por la AA, y sus requisitos se describen en el punto 6.2.1

7.PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1 Perfil de certificado

Todos los certificados emitidos por la CA de DOCUMENTA S.A., deberán estar conformes al formato definido por la norma ITU X.509 o ISO/IEC 9594-8.

A continuación, se detalla el contenido de las extensiones más significativas de los certificados de firma digital del tipo F2 emitidos por la CA de DOCUMENTA S.A.

a) Certificado de Persona Física del tipo F2

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

SUJETO del Certificado de Persona Física del tipo F2		
Campo	**Valor de Ejemplo**	**Descripción**
Country (C) {OID: 2.5.4.6}	PY	Código de país es asignado de acuerdo al estándar ISO 3166

Organization (O) {OID: 2.5.4.10}	**PERSONA FISICA**	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y se debe indicar PERSONA FISICA, en mayúscula y sin tilde.
Organization Unit (OU) {OID: 2.5.4.11}	**FIRMA F2**	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En este caso se identifica que corresponde a un certificado emitido en módulo hardware y se debe indicar FIRMA F2, en mayúscula.
Common Name (CN) {OID: 2.5.4.3}	**JAVIER ARMANDO DOMINGUEZ TALAVERA**	Este campo debe contener el/los nombre/s y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {OID: 2.5.4.5}	**CI8426243**	**CI** más Número de Cédula de Identidad del titular del certificado, según documento de identificación
GivenName (G) {OID: 2.5.4.42}	**JAVIER ARMANDO**	Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Surname (SN) {OID: 2.5.4.4}	**DOMINGUEZ TALAVERA**	Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.

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

NOMBRE ALTERNATIVO DEL SUJETO del Certificado de Persona Física del tipo F2		
Campo	**Valor de Ejemplo**	**Descripción**
Rfc822Name	javierdominguez@hmail.com	Email del titular del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.10}	O = BLANCO S.A.	Nombre de la organización en el que presta servicio el titular del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.11}	OU = AREA TECNICA	Nombre de la unidad de la organización en el que presta servicio el titular del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.5}	SerialNumber = RUC800561-3	**RUC** más Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado.
DirectoryName {OID: 2.5.4.12}	T= DIRECTOR TECNICO	Cargo o Titulo del titular del certificado. Campo no obligatorio.

Los otros campos que compone la extensión “Subject Alternative Name” podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuando estén aprobados por la CA Raíz.

Descripción del resto de campos más relevantes del perfil de certificado de persona física del tipo F2:

CAMPO	COMPONENTE PROPUESTO	CRITI CA
1. Versión	V3	
2. Serial Number	**[NÚMERO DE SERIE DEL CERTIFICADO DIGITAL. VALOR ÚNICO EMITIDO DENTRO DEL ÁMBITO DE LA CA DE DOCUMENTA S.A.]**	
3. Signature Algorithm	sha256WithRSAEncryption	
4. Signature Hash Algorithm	sha256	
5. Issuer	CN = CA-DOCUMENTA S.A. O = DOCUMENTA S.A. C = PY SERIALNUMBER = RUC 80050172-1	

6. Validez	**[PUEDE SER HASTA 2 AÑOS]**	
7. Subject	**C = [CÓDIGO DE PAÍS ES ASIGANDO DE ACUERDO AL ESTANDAR ISO 3166]** **O = PERSONA FISICA** **OU = FIRMA F2** **CN = [NOMBRES Y APELLIDOS DEL TITULAR, SEGÚN DOCUMENTO DE IDENTIFICACIÓN, EN MAYÚSCULAS Y SIN TILDES, A EXCEPCIÓN DE LA Ñ. PODRÁN SER INCLUIDOS DIERESIS Y APÓSTROFES SI CORRESPONDE.]** **SERIALNUMBER = [SIGLAS CI MÁS NÚMERO DE CÉDULA DE IDENTIDAD DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO DE IDENTIFICACIÓN]** **G = [SE REGISTRA EL NOMBRE DEL TITULAR, SEGÚN DOCUMENTO DE IDENTIFICACIÓN, EN MAYÚSCULAS Y SIN TILDES, A EXCEPCIÓN DE LA Ñ. PODRÁN SER INCLUIDOS DIERESIS Y APÓSTROFES SI CORRESPONDE.]** **SN = [SE REGISTRA EL APELLIDO DEL TITULAR, SEGÚN DOCUMENTO DE IDENTIFICACIÓN, EN MAYÚSCULAS Y SIN TILDES, A EXCEPCIÓN DE LA Ñ. PODRÁN SER INCLUIDOS DIERESIS Y APÓSTROFES SI CORRESPONDE.]**	
8. Subject Public Key Info	**Algoritmo: RSA Encryption** **Longitud: 2048 bits o 4096 bits**	
9. Certificate Policies **. Policy Identifier** **.URL CPS** **. Notice Referente**	**Se utilizará** **1.3.6.1.4.1.48315.1.1.1.6.1.1** **https://www.documenta.com.py/firmadigital/descargas** **Este es un certificado de persona física cuya clave privada está contenida en un módulo de hardware seguro cuya finalidad es autenticar a su titular o generar firmas digitales.**	NO
10. CRLDistributionPoints	**https://www.documenta.com.py/firmadigital/descargas/crldoc.crl**	NO
11. Auth. Information Access **. CAIssuers** **. OCSP**	**Se utilizará** **https://www.documenta.com.py/firmadigital/descargas/cadoc.crt** **http://www.documenta.com.py/firmadigital/oscp**	NO
12. KeyUsage	**Firma Digital (Digital Signature)** **Cifrado de Clave (Key Encipherment)** **No Repudio (Non Repudiation)**	**SI**
13. extKeyUsage	**Correo Seguro** **Autenticación del cliente** **Autenticación del servidor**	SI

14. Subject Alternative Name	**RFC822Name = [EMAIL DEL TITULAR DEL CERTIFICADO]** **. DirectoryName** **O = [2.5.4.10: NOMBRE DE LA ORGANIZACIÓN EN EL QUE PRESTA SERVICIO EL TITULAR DEL CERTIFICADO]** **OU = [2.5.4.11: NOMBRE DE LA UNIDAD DE LA ORGANIZACIÓN EN EL QUE PRESTA SERVICIO EL TITULAR DEL CERTIFICADO]** **SERIALNUMBER = [2.5.4.5: SIGLAS RUC MÁS NÚMERO DE CÉDULA TRIBUTARIA CORRESPONDIENTE A LA ORGANIZACIÓN EN EL QUE PRESTA SERVICIO EL TITULAR DEL CERTIFICADO** **T = [2.5.4.12: [CARGO O TITULO DEL TITULAR DEL CERTIFICADO]**	NO
15. Subject Key Identifier	**SHA-1 hash de la clave pública**	NO
16. Authority Key Identifier **. KeyIdentifier** **. AuthorityCertIssuer** **. AuthorityCertSerialNumber**	**Se utilizará** **SHA-1 hash de la clave pública del emisor** **No utilizado** **No utilizado**	NO

b) Certificado de Persona Jurídica del tipo F2

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

SUJETO del Certificado de Persona Jurídica del tipo F2		
Campo	**Valor de Ejemplo**	**Descripción**
Country (C) {OID: 2.5.4.6}	**PY**	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O) {OID: 2.5.4.10}	**PERSONA JURIDICA**	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona jurídica y se debe indicar PERSONA JURIDICA, en mayúscula y sin tilde.

Organization Unit (OU) {OID: 2.5.4.11}	FIRMA F2	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En este caso se identifica que corresponde a un certificado emitido en módulo software y se debe indicar FIRMA F2, en mayúscula.
Common Name (CN) {OID: 2.5.4.3}	EMPRESA S.A.	Este campo debe contener la razón social del titular del certificado, según documento identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {OID: 2.5.4.5}	RUC620032-2	**RUC** más número de cédula tributaria del titular del certificado, según documento de identificación.

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

NOMBRE ALTERNATIVO DEL SUJETO del Certificado de Persona Jurídica del tipo F2		
Campo	**Valor de Ejemplo**	**Descripción**
Rfc822Name	empresasa@hmail.com	Email del titular del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.3}	CN = JAVIER DOMINGUEZ	Nombre y apellido del responsable del certificado. Campo obligatorio.
DirectoryName {OID: 2.5.4.5}	SerialNumber = CI800563	**CI** más Número de cédula de identidad correspondiente al responsable del certificado. Campo obligatorio.
DirectoryName {OID: 2.5.4.12}	T= REPRESENTANTE LEGAL	Cargo que ocupa en la organización el responsable del certificado. Campo no obligatorio.

Los otros campos que compone la extensión “Subject Alternative Name” podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuando estén aprobados por la CA Raíz.

Descripción del resto de campos más relevantes del perfil de certificado de persona jurídica del tipo F2:

CAMPO	COMPONENTE PROPUESTO	CRITI CA
1. Versión	**V3**	
2. Serial Number	**[NÚMERO DE SERIE DEL CERTIFICADO DIGITAL. VALOR ÚNICO EMITIDO DENTRO DEL ÁMBITO DE LA CA DE DOCUMENTA S.A.]**	
3. Signature Algorithm	**sha256WithRSAEncryption**	
4. Signature Hash Algorithm	**sha256**	
5. Issuer	**CN = CA-DOCUMENTA S.A.** **O = DOCUMENTA S.A.** **C = PY** **SERIALNUMBER = RUC 80050172-1**	
6. Validez	**[PUEDE SER HASTA 2 AÑOS]**	
7. Subject	**C = [CÓDIGO DE PAÍS ES ASIGANDO DE ACUERDO AL ESTANDAR ISO 3166]** **O = PERSONA JURIDICA** **OU = FIRMA F2** **CN = [SE REGISTRA LA RAZÓN SOCIAL DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO IDENTIFICACIÓN, EN MAYÚSCULAS Y SIN TILDES, A EXCEPCIÓN DE LA Ñ. PODRÁN SER INCLUIDOS DIÉRESIS Y APOSTROFES SI CORRESPONDE.]** **SERIALNUMBER = [SIGLAS RUC MÁS NÚMERO DE CÉDULA TRIBUTARIA DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO DE IDENTIFICACIÓN]**	
8. Subject Public Key Info	**Algoritmo: RSA Encryption** **Longitud: 2048 bits o 4096 bits**	
9. Certificate Policies **. Policy Identifier** **.URL CPS** **. Notice Referente**	**Se utilizará** **1.3.6.1.4.1.48315.1.1.1.6.2.1** **https://www.documenta.com.py/firmadigital/descargas** **Este es un certificado de persona jurídica cuya clave privada está contenida en un módulo de hardware seguro cuya finalidad es autenticar a su titular o generar firmas digitales.**	NO
10. CRLDistributionPoints	**https://www.documenta.com.py/firmadigital/descargas/crldoc.crl**	NO
11. Auth. Information Access **. CAIssuers**	**Se utilizará** **https://www.documenta.com.py/firmadigital/descargas/cadoc.crt**	NO

. OCSP	http://www.documenta.com.py/firmadigital/oscp	
12. KeyUsage	Firma Digital (Digital Signature) Cifrado de Clave (Key Encipherment) No Repudio (Non Repudiation)	**SI**
13. extKeyUsage	Correo Seguro Autenticación del cliente Autenticación del servidor	SI
14. Subject Alternative Name **. No Obligatorio:** **. Obligatorio:**	 RFC822Name = **[EMAIL DEL TITULAR DEL CERTIFICADO]** **. DirectoryName** T = **[2.5.4.12: CARGO O QUE OCUPA EN LA ORGANIZACIÓN EL TITULAR DEL CERTIFICADO]** CN = **[2.5.4.3: NOMBRES Y APELLIDOS DEL RESPONSABLE DEL CERTIFICADO]** SERIALNUMBER = **[2.5.4.5: SIGLAS CI MÁS NÚMERO DE CÉDULA DE IDENTIDAD CORRESPONDIENTE AL RESPONSIBLE DEL CERTIFICADO**	NO
15. Subject Key Identifier	SHA-1 hash de la clave pública	NO
16. Authority Key Identifier **. KeyIdentifier** **. AuthorityCertIssuer** **. AuthorityCertSerialNumber**	**Se utilizará** **SHA-1 hash de la clave pública del emisor** **No utilizado** **No utilizado**	NO

c) Certificado de Máquina o Aplicación del tipo F2

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

SUJETO del Certificado de Máquina o Aplicación del tipo F2		
Campo	**Valor de Ejemplo**	**Descripción**
Country (C) {OID: 2.5.4.6}	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O) {OID: 2.5.4.10}	APLICACIÓN	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de máquina o aplicación y puede ser MAQUINA O APLICACION, en mayúscula y sin tilde.
Organization Unit (OU) {OID: 2.5.4.11}	FIRMA F2	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En este caso se identifica que corresponde a un certificado emitido en módulo hardware y se debe indicar FIRMA F2, en mayúscula.
Common Name (CN) {OID: 2.5.4.3}	APLICATION CERT	Este campo debe contener la URL correspondiente o el nombre de la aplicación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.
Serial Number {OID: 2.5.4.5}	MRUC4564-2	Este campo debe contener según sea el titular: - Persona Física: Las siglas MCI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación. - Persona Jurídica: Siglas MRUC, seguidas del número de cédula tributaria, según el documento de identificación.

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

NOMBRE ALTERNATIVO DEL SUJETO del Certificado de Persona Jurídica del tipo F2		
Campo	**Valor de Ejemplo**	**Descripción**
Rfc822Name	javierdominguez@hmail.com	Email del responsable del certificado. Campo no obligatorio.
DirectoryName {OID: 2.5.4.3}	O = EMPRESA S.A.	Si se trata de una Persona Jurídica, nombre de la organización titular del certificado. Campo obligatorio
DirectoryName {OID: 2.5.4.3}	CN = JAVIER DOMINGUEZ	Nombre y apellido del responsable del certificado. Campo obligatorio.
DirectoryName {OID: 2.5.4.5}	SerialNumber = CI800563	Si se trata de una Persona Jurídica, **CI** más número de cédula de identidad correspondiente al responsable del certificado. Campo obligatorio.
DirectoryName {OID: 2.5.4.12}	T= REPRESENTANTE LEGAL	Si se trata de una Persona Jurídica, cargo que ocupa en la organización el responsable del certificado. Campo no obligatorio.

Los otros campos que compone la extensión “Subject Alternative Name” podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuando estén aprobados por la CA Raíz.

Descripción del resto de campos más relevantes del perfil de certificado de persona jurídica del tipo F2:

CAMPO	COMPONENTE PROPUESTO	CRITI CA
1. Versión	V3	
2. Serial Number	**[NÚMERO DE SERIE DEL CERTIFICADO DIGITAL. VALOR ÚNICO EMITIDO DENTRO DEL ÁMBITO DE LA CA DE DOCUMENTA S.A.]**	
3. Signature Algorithm	sha256WithRSAEncryption	
4. Signature Hash Algorithm	sha256	
5. Issuer	CN = CA-DOCUMENTA S.A. O = DOCUMENTA S.A. C = PY SERIALNUMBER = RUC 80050172-1	

6. Validez	**[PUEDE SER HASTA 2 AÑOS]**	
7. Subject	**C = [CÓDIGO DE PAÍS ES ASIGANDO DE ACUERDO AL ESTANDAR ISO 3166]** **O = [MAQUINA O APLICACION]** **OU = FIRMA F2** **CN = [SE REGISTRA LA URL CORRESPONDIENTE O EL NOMBRE DE LA APLICACIÓN, EN MAYÚSCULAS Y SIN TILDES, A EXCEPCIÓN DE LA Ñ. PODRÁN SER INCLUIDOS DIÉRESIS Y APOSTROFES SI CORRESPONDE.]** **SERIALNUMBER = [SIGLAS MRUC MÁS NÚMERO DE CÉDULA TRIBUTARIA DEL TITULAR DEL CERTIFICADO, O MCI MÁS NÚMERO DE CÉDULA DE IDENTIDAD, SEGÚN DOCUMENTO DE IDENTIFICACIÓN]**	
8. Subject Public Key Info	**Algoritmo: RSA Encryption** **Longitud: 2048 bits o 4096 bits**	
9. Certificate Policies **. Policy Identifier** **.URL CPS** **. Notice Referente**	**Se utilizará** **1.3.6.1.4.1.48315.1.1.1.6.3.1** **https://www.documenta.com.py/firmadigital/descargas** **Este es un certificado de máquina o aplicación cuya clave privada está contenida en un módulo de hardware seguro cuya finalidad es autenticar a su titular o generar firmas digitales.**	NO
10. CRLDistributionPoints	**https://www.documenta.com.py/firmadigital/descargas/crldoc.crl**	NO
11. Auth. Information Access **. CAIssuers** **. OCSP**	**Se utilizará** **https://www.documenta.com.py/firmadigital/descargas/cadoc.crt** **http://www.documenta.com.py/firmadigital/oscp**	NO
12. KeyUsage	**Firma Digital (Digital Signature)** **Cifrado de Clave (Key Encipherment)** **No Repudio (Non Repudiation)**	**SI**
13. extKeyUsage	**Correo Seguro** **Autenticación del cliente** **Autenticación del servidor**	SI

14. Subject Alternative Name **. No Obligatorio:** **. Obligatorio:**	 **RFC822Name = [EMAIL DEL TITULAR DEL CERTIFICADO]** **. DirectoryName** **T = [2.5.4.12: CARGO O QUE OCUPA EN LA ORGANIZACIÓN EL RESPONSABLE DEL CERTIFICADO]** **CN = [2.5.4.3: NOMBRES Y APELLIDOS DEL RESPONSABLE DEL CERTIFICADO]** **O = [2.5.4.10: NOMBRE DE LA ORGANIZACIÓN TITULAR DEL CERTIFICADO]** **SERIALNUMBER = [2.5.4.5: SIGLAS CI MÁS NÚMERO DE CÉDULA DE IDENTIDAD CORRESPONDIENTE AL RESPONSABLE DEL CERTIFICADO**	NO
15. Subject Key Identifier	**SHA-1 hash de la clave pública**	NO
16. Authority Key Identifier **. KeyIdentifier** **. AuthorityCertIssuer** **. AuthorityCertSerialNumber**	**Se utilizará** **SHA-1 hash de la clave pública del emisor** **No utilizado** **No utilizado**	NO

7.1.1 Número de versión

La PKI de DOCUMENTA S.A. soporta y utiliza certificados X.509 versión 3 (X.509 v3) de acuerdo con el perfil establecido con el RFC 5280.

7.1.2 Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- KeyUsage. **Calificada como crítica.**
- ExtendedKeyUsage. **Calificada como crítica**
- CertificatePolicies. **Calificada como no crítica.**
- SubjectAlternativeName. **Calificada como no crítica.**
- Authority Information Access. **Calificada como no crítica**
- CRLDistributionPoint. **Calificada como no crítica.**

El contenido de las extensiones más significativas de los certificados emitidos se encuentra en el Ítem 7.1

7.1.3 Identificadores de objeto de algoritmos

Los certificados generados dentro de la PKI Paraguay deben usar el siguiente algoritmo:

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 Formas del nombre

Los nombres del titular del certificado, que consta en el campo "*Subject*" y el número de identificación, que consta el campo "Serial Number", deberán adoptar el "*Distinguished Name"* (DN) del estándar ITU X.500/ISO 9594.

7.1.5 Restricciones del nombre

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

Los nombres se escriben en mayúsculas y sin tildes.

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 de política de certificado

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

7.1.7 Uso de la extensión restricciones de política (POLICY CONSTRAINTS)

No estipulado.

7.1.8 Semántica y sintaxis de los calificadores de política (POLICY QUALIFIERS)

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: Contiene 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)

Extensiones críticas deben ser interpretadas conforme a la RFC

5280.

7.2 Perfil de CRL

Como establezca la CPS de la CA de DOCUMENTA S.A.

7.2.1 Número (s) de versión

Como establezca la CPS de la CA de DOCUMENTA S.A.

7.2.2 CRL y extensiones de entradas de CRL

Como establezca la CPS de la CA de DOCUMENTA S.A.

7.3 Perfil de OCSP

Como establezca la CPS de la CA de DOCUMENTA S.A.

7.3.1 Número(s) de versión

Como establezca la CPS de la CA de DOCUMENTA S.A.

7.3.2 Extensiones OCSP

Como establezca la CPS de la CA de DOCUMENTA S.A.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 Frecuencia o circunstancias de evaluación

Como establezca la CPS de la CA de DOCUMENTA S.A.

8.2 Identificación/calificación del evaluador

Como establezca la CPS de la CA de DOCUMENTA S.A.

8.3 Relación del evaluador con la entidad evaluada

Como establezca la CPS de la CA de DOCUMENTA S.A.

8.4 Aspectos cubiertos por la evaluación

Como establezca la CPS de la CA de DOCUMENTA S.A.

8.5 Acciones tomadas como resultado de una deficiencia

Como establezca la CPS de la CA de DOCUMENTA S.A.

8.6 Comunicación de resultados

Como establezca la CPS de la CA de DOCUMENTA S.A.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

9.1.1 Tarifas de emisión y administración de certificados

DOCUMENTA S.A. se encuentra obligado a cumplir con las tasas y aranceles impuestos por la normativa vigente.

DOCUMENTA S.A. deberá comunicar al interesado en adquirir un

certificado digital de todos los costos que deberá asumir para la obtención del certificado.

9.1.2 Tarifas de acceso a certificados

La CA de DOCUMENTA S.A., no se encuentra habilitada para el cobro de tarifas de acceso a certificados.

9.1.3 Tarifas de acceso a información del estado o revocación

La CA de DOCUMENTA S.A., no se encuentra habilitada para el cobro de tarifas de acceso a estado o revocación de los certificados.

9.1.4 Tarifas por otros servicios

La CA de DOCUMENTA S.A., no se encuentra habilitada para el cobro de tarifas para acceder a información de las Políticas de Certificación y la Declaración de Prácticas de Certificación de DOCUMENTA S.A.

9.1.5 Políticas de reembolso

Si el certificado del titular debe ser revocada debido a compromiso de clave privada de la CA de DOCUMENTA S.A., o cuando se constatan errores en el certificado digital o en el procedimiento de emisión, atribuibles a la CA de DOCUMENTA S.A. o a sus RA vinculadas, se emitirá otro certificado de reemplazo sin cargo.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.2.2 Otros activos

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.2.3 Cobertura de seguro o garantía para usuarios finales

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.3 Confidencialidad de la información comercial

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.3.1 Alcance de la información confidencial

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.3.2 Información no contenida en el alcance de información confidencial

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.4 Privacidad de información personal

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.4.1 Plan de privacidad

Como establezca la CPS de la CA de DOCUMENTA S.A

9.4.2 Información tratada como privada

Como establezca la CPS de la CA de DOCUMENTA S.A

9.4.3 Información que no es considerada como privada

Como establezca la CPS de la CA de DOCUMENTA S.A

9.4.4 Responsabilidad para proteger información privada

Como establezca la CPS de la CA de DOCUMENTA S.A

9.4.5 Notificación y consentimiento para usar información privada

Como establezca la CPS de la CA de DOCUMENTA S.A

9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo.

Como establezca la CPS de la CA de DOCUMENTA S.A

9.4.7 Otras circunstancias de divulgación de información

Como establezca la CPS de la CA de DOCUMENTA S.A

9.5 Derecho de propiedad intelectual

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6 Representaciones y garantías

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6.1 Representaciones y garantías de la CA

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6.2 Representaciones y garantías de la RA

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6.3 Representaciones y garantías del suscriptor

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6.4 Representaciones y garantías de las partes que confían

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6.5 Representaciones y garantías del repositorio

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.6.6 Representaciones y garantías de otros participantes

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.7 Exención de garantías

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.8 Limitaciones de responsabilidad legal

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.9 Indemnizaciones

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.10 Plazo y finalización

9.10.1 Plazo

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

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

9.10.2 Finalización

Esta CP 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 CP 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 y supervivencia

Las obligaciones y restricciones que establece esta CP, 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 Notificación individual y comunicaciones con participantes

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.12 Enmiendas

9.12.1 Procedimientos para enmiendas

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.12.2 Procedimiento de publicación y notificación

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.12.3 Circunstancias en los OID deben ser cambiados

Sin estipulaciones.

9.13 Disposiciones para resolución de disputas

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.14 Normativa aplicable

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.15 Adecuación a la ley aplicable

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

9.16 Disposiciones varias

9.16.1 Acuerdo completo

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.16.2 Asignación

Sin estipulaciones.

9.16.3 Divisibilidad

En el caso de que una o más cláusulas de esta CP 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

Como establezca la CPS de la CA de DOCUMENTA S.A.

9.17 Otras disposiciones

Como establezca la CPS de la CA de DOCUMENTA S.A.

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.
- Directivas Obligatorias Para La Formulación y Elaboración De La Política de Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Directivas Obligatorias Para La Formulación y Elaboración De La Práctica De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Características Mínimas De Seguridad Para La Autoridades De Registro De La Infraestructura De Claves Públicas Del Paraguay V 1.0
- Normas de Algoritmos Criptográficos PKI-Paraguay V1.0

ANEXO 1

Tabla Comparativa de requisitos mínimos por tipo de certificado.

Tipo de Certificado	Clave criptográfica			Validez máxima del certificado	Frecuencia de emisión del CRL (horas)	Tiempo límite de revocación (horas)
	Tamaño (bits)	Proceso de generación	Medio de almacenamiento			
F1	RSA 2048	Software	1. Repositorio protegido por contraseña y/o identificación biométrica, cifrado por software. 2. Tarjeta Inteligente, token o HSM, sin capacidad de generación de clave y protegido por contraseña y/o identificación biométrica.	1	12	12
F2	RSA 2048, 4096	Hardware	1. Tarjeta Inteligente, token o HSM, sin capacidad de generación de clave y protegido por contraseña y/o identificación biométrica.	2	12	12