CONTROL DOCUMENTAL

DOCUMENTO	
Titulo: Política de Certificación de Persona Física 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-CPFv1.0.0	
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 **POLITICA DE CERTIFICACION DE PERSONA FISICA** 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.

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 Persona Física de la CA 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/cpf.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 CP 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 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 de 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 la CA de DOCUMENTA 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 CP, los Terceros que confían son las personas o entidades diferentes del titular que deciden aceptar y confiar en los certificados emitidos por 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

Los certificados regulados por la presente PC sólo deben utilizarse con el propósito de **autenticación o firma** de personas físicas. Para determinar si es posible utilizar un certificado de persona física para autenticación o un certificado de persona

física para firma digital 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 persona física para firma digital.	Firma digital • No repudio (Non-Repudiation)
Certificado de persona física para autenticación.	Autenticación • Firma Digital (Digital Signature) • Cifrado de Clave (Key Encipherment)

1.4.2. Usos prohibidos del certificado

Los certificados de persona física no deben emplearse para ninguna actividad no especificada en el punto anterior.

1.5. Administración de las Políticas

1.5.1. Organización que administra el documento

Como establezca la CPS de DOCUMENTA S. A.

1.5.2. Persona de Contacto

Como establezca la CPS de DOCUMENTA S. A.

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

Como establezca la CPS de DOCUMENTA S. A.

1.5.4. Procedimientos de aprobación de la Política de Certificación (CP)

Como establezca la CPS de DOCUMENTA S. A.

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.

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

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 a los Repositorios

Como establezca la CPS de DOCUMENTA S. A.

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 de los nombres distintivos para los certificados de persona física de la Infraestructura de Claves Publicas del Paraguay:

NOMBRE DISTITIVO del Certificado de Persona Física		
Campo	**Valor de Ejemplo**	**Descripción**
Country (C)	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	RAFAEL DANIEL ROMERO LLANO	Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes. Únicamente se debe aceptar el carácter ‘’Ñ ‘’como un caso especial para los nombres de personas físicas.
Organization Unit (OU)	PERSONA FISICA	La Política identifica si se trata de un certificado para: **PERSONA FÍSICA** o **PERSONA JURÍDICA.**
Common Name (CN)	RAFAEL DANIEL ROMERO LLANO (FIRMA)	Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes. Únicamente se debe aceptar el carácter ‘’Ñ ‘’como un caso especial para los nombres de personas físicas.El propósito debe ser **FIRMA** o **AUTENTICACION**

Serial Number **{OID: 2.5.4.5}**	**CI 8484263**	**CI** más Número de Cédula de Identidad para paraguayos o **CIE** más Cédula de identidad para extranjeros
Surname (SN) **{OID: 2.5.4.4}**	**ROMERO LLANO**	Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes. Únicamente se debe aceptar el carácter ''Ñ ''como un caso especial para los nombres de personas físicas.
GivenName (G) **{OID:2.5.4.42}**	**RAFAEL DANIEL**	Se registra el nombre de suscriptor, en mayúsculas y sin tildes Únicamente se debe aceptar el carácter ''Ñ ''como un caso especial para los nombres de personas físicas.

3.1.2 Necesidad de Nombres significativos

En todos los casos el nombre distintivo del titular del certificado debe ser significativo, ajustándose a las normas impuestas en el apartado anterior.

El nombre significativo, corresponde al especificado en el documento de identificación presentado por el solicitante en el momento de registro.

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 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 Persona Física para firma digital y Certificado de Persona Física para para autenticación

La Cédula de identidad es expedida por el Departamento de Identificaciones de la Policía Nacional, y deben cumplir el siguiente formato en el sub campo Serial Number (Número de Serie):

Tipo de Documento	Prefijo	Formato
Cédula de identidad Policial	CI	CI 9999999
Cédula de identidad Policial para extranjero	CIE	CIE 9999999

3.1.5 Unicidad de los nombres

El conjunto de nombre distintivo (Distinguished Name) debe ser único y no ambiguo. El uso del número de cédula de identidad en el "**Serial Number (Número de Serie)**"más el sufijo **"Autenticación"** para el certificado de persona física para autenticación o el sufijo **"Firma"** para el de certificado de persona física para firma digital en el campo "**Common Name (Nombre Común)",** garantiza la unicidad del mismo.

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 CP.

3.1.7 Reconocimiento, autenticación y rol de las marcas registradas

Como establezca la CPS de DOCUMENTA S. A.

3.2 Validación inicial de la identidad

3.2.1 Medio de prueba de posesión de la clave privada

Las claves de los certificados de persona física serán generadas por el titular de las mismas por lo que 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 la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 Autenticación de la identidad de una persona jurídica

No estipulado.

3.2.3 Autenticación de la identidad de una persona física

El solicitante de certificados de persona física deberá proporcionar la siguiente información:

Datos personales:

- Primer nombre.
- Segundo nombre.
- Primer apellido.
- Segundo apellido
- Cédula de identidad
- Dirección de correo electrónico
- Fecha de nacimiento

Para poder autenticar la identidad de la persona física, el solicitante deberá comparecer en el puesto de inscripción de la RA de DOCUMENTA S. A. con su cédula de identidad. Además, de los datos proporcionados en la solicitud, en el puesto de inscripción se podrán capturarán los datos biométricos del solicitante.

3.2.4 Información no verificada sobre el solicitante

No estipulado.

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. Se validará:

- el nombre y documento de identidad.
- la mayoría de edad.

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

3.2.6 Criterios para operar con CA externas

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 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

Los procedimientos aceptados para la autenticación del solicitante de la revocación incluyen algunos de los siguientes medios:

- Mediante el código de revocación que es enviado al suscriptor en el correo consignado en el momento de la emisión del certificado.
- Presencialmente a través de los procesos de autenticación, de identidad (secciones 3.2.2. y 3.2.3.)
- Cualquier otro medio establecido por DOCUMENTA S. A. y aprobado por el MIC que permita una identificación veraz y segura

Los sujetos habilitados para solicitar la revocación se encuentran establecidos en la sección 4.9.2 y los procedimientos de revocación en la sección 4.9.3.

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

4.1 Solicitud de certificados

4.1.1 Quién puede efectuar una solicitud

La solicitud de certificado de persona física será efectuada por la persona física que vaya a ser titular del mismo. Para ello, el solicitante deberá comparecer en el puesto de inscripción de la RA de DOCUMENTA S. A

4.1.2 Proceso de Inscripción y responsabilidades

El procedimiento de solicitud de certificados de persona física es el siguiente:

1. La persona física que será titular del certificado a emitir solicita una cita en uno de los puestos de RA de Documenta S. A. al correo firmadigital@documenta.com.py. Para obtener una cita, la información que debe aportar el solicitante es la siguiente:

a. Datos personales de acuerdo a lo que figura en su cédula de identidad:

- Primer nombre.
- Segundo nombre.
- Primer apellido.
- Segundo apellido
- Número de cédula de identidad personal
- Dirección de correo electrónico
- Fecha de nacimiento

2. El día y hora a la que el solicitante tenga su cita deberá presentarse en el puesto de inscripción de la RA de DOCUMENTA S. A., identificándose mediante su cédula de identidad personal más otro documento adicional que confirme la identidad del mismo. El documento adicional podrá ser pasaporte, certificado de nacimiento, registro de conducir, antecedente policial o antecedente judicial. En el puesto de inscripción se podrán capturar el registro de los datos biométricos del solicitante. Posteriormente se entrega el dispositivo criptográfico sin certificados

3. Una vez que el solicitante haya obtenido su dispositivo criptográfico, en el puesto de emisión de la RA de DOCUMENTA S. A. se procederá a la generación de sus certificados en el dispositivo criptográfico que acaba de obtener el solicitante. Por último se procede a la firma del acuerdo de suscriptores.

Es responsabilidad del solicitante garantizar la completitud y veracidad de toda la información aportada para obtener sus certificados de persona física con independencia de las comprobaciones realizadas por el prestador de servicios de certificación para verificarla.

4.2 Procesamiento de la Solicitud del Certificado

4.2.1 Realización de las funciones de identificación y autenticación

La realización de las funciones de identificación y autenticación requerirá la presencia física del solicitante junto con su cédula de identificación personal en el puesto de inscripción de la RA. En el puesto de emisión de la RA, la identificación y autenticación del usuario se realizará con el dispositivo criptográfico que éste ha obtenido en el puesto de inscripción de la RA.

El proceso de identificación y autenticación de un solicitante está descrito en el apartado 3.2.3 del presente documento.

4.2.2 Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que la CA de 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 el apartado anterior.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

Se establece el plazo máximo de cinco días hábiles para la tramitación de la solicitud del certificado, contados a partir de haberse verificado la identidad del solicitante y admitida la solicitud.

En caso que la CA de DOCUMENTA S. A. supere el plazo máximo establecido para la tramitación de la solicitud, deberá informar al solicitante de las causas que motivaron la demora y el nuevo plazo en el que se tramitará la solicitud. En caso que el interesado opte por desistir de su solicitud por el motivo expuesto, DOCUMENTA S. A. accederá al reembolso de lo abonado.

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 de DOCUMENTA S.A. Cuando se emita un certificado de acuerdo con una solicitud de certificación se

efectuará las notificaciones que se establecen en el apartado 4.3.2 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.

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

El envío de la notificación al solicitante se realizará por medio del correo electrónico provisto por éste durante la inscripción de sus datos, previa a la emisión del certificado.

4.4 Aceptación del certificado

4.4.1 Mecanismo de aceptación del certificado

Los titulares de los certificados de persona física, deberán aceptar los términos y condiciones contenidos en el acuerdo de suscriptores de la CA de DOCUMENTA S. A. mediante una firma manuscrita o digital.

4.4.2 Publicación del certificado por la CA

Documenta S. A. publicará información de los certificados que emite a través de un mecanismo de consulta que estará disponible en el sitio principal de Internet.

Además DOCUMENTA S. A. publica en su repositorio público su certificado digital y el de la CA raíz.

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

Cuando la CA de DOCUMENTA S. A. emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, enviará una copia del mismo a la RA que remitió la solicitud.

4.5 Par de claves y uso del certificado

Los Certificados de Persona Física son certificados de uso intransferible que acreditan la identidad de su titular.

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

El titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en esta 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 la realización de funciones que requieran acreditar la identidad del titular como persona física.

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 la realización de funciones que requieran acreditar la identidad del titular como persona física 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 la CPS de la CA de DOCUMENTA S. A. y en la presente CP.

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 CP, cuando un certificado requiera ser renovado debe solicitarse uno nuevo, de acuerdo con la sección 4.1 de esta CP.

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 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 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 CP.

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.

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 CPS asociada o de la presente CP.
- Por fallecimiento, ausencia legalmente declarada, incapacidad total o parcial de la persona física.
- 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 esta CP.

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 CP 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 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.

4.9.3 Procedimiento de solicitud de revocación

La solicitud de revocación de los certificados de persona física podrá efectuar el titular de los mismos de las siguientes maneras:

- presencial en el puesto de inscripción de la RA de DOCUMENTA S. A., identificándose según lo establecido en el punto 4.1.2 paso 2 de la presente CP.
- Remota ingresando al portal web habilitado para el efecto. El enlace de acceso al portal de revocación y la clave de revocación, serán enviados en el correo electrónico consignado por el titular en el formulario de solicitud de emisión del certificado.

En los casos que la solicitud de revocación provenga de una Autoridad Judicial Competente o un tercero, la CA de DOCUMENTA S. A. deberá evaluar la solicitud. Antes de comenzar con el proceso de revocación se deberá notificar al suscriptor lo cual no implicará aun la revocación efectiva del certificado.

Un certificado revocado será válido únicamente para la verificación de firmas generadas durante el periodo en que el referido certificado era válido.

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

Las solicitudes de revocación deben resolverse tan rápido como sea posible en un tiempo no superior a 24 horas.

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

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

4.9.7 Frecuencia de emisión de CRL

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

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

El tiempo máximo entre la generación de una CRL y su correspondiente publicación en el repositorio es de 1 hora.

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

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

4.9.10 Requisitos de comprobación en línea de revocación

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

4.9.11 Otras formas de divulgación de información de revocación disponibles

No estipulado.

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

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 adicionales

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

4.11 Extinción de la validez de un certificado

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

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de custodia y recuperación de claves

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

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

5.1 Controles físicos

5.1.1 Ubicación física y construcción

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 Alimentación eléctrica y aire acondicionado

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

5.1.4 Exposición al agua

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

5.1.5 Prevención y protección frente a incendios

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

5.1.6 Sistema de almacenamiento

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 Copias de seguridad fuera de las instalaciones

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

5.2 Controles de procedimiento

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

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 Roles que requieren segregación de funciones

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

5.3 Controles de personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

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

5.3.2 Procedimientos de comprobación de antecedentes

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

5.3.3 Requerimientos de formación

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

5.3.4 Requerimientos y frecuencia de actualización de la formación

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

5.3.5 Frecuencia y secuencia de rotación de tareas

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

5.3.6 Sanciones por actuaciones no autorizadas

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

5.3.7 Requisitos de contratación de terceros

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

5.3.8 Documentación proporcionada al personal

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

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

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

5.4.2 Frecuencia de procesado de registros de auditoría

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

5.4.3 Periodo de conservación de los registros de auditoría

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

5.4.4 Protección de los registros de auditoría

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

5.4.5 Procedimientos de respaldo de los registros de auditoría

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

5.4.6 Notificación al sujeto causa del evento

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

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

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

5.5 Archivado de registros

5.5.1 Tipo de eventos archivados

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

5.5.2 Periodo de conservación de registros

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

5.5.3 Protección del archivo

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

5.5.4 Procedimientos de copia de respaldo del archivo

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

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)

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 claves

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

5.7 Recuperación ante compromiso de clave o catástrofe

5.7.1 Procedimientos de gestión de incidentes y compromisos

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

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

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

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

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.

5.8 Cese de una PSC o RA

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

Los pares de claves para los certificados de persona física se generan en dispositivos criptográficos hardware con certificación FIPS 140-2 Nivel 2 o superior.

6.1.2 Entrega de la clave privada al titular

La clave privada de los certificados de persona física es generada por el propio titular en su dispositivo criptográfico, por lo que en ningún caso será entregada al mismo.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública de los certificados de persona física se genera en el dispositivo criptográfico del titular en el puesto de emisión siendo la RA de DOCUMENTA S. A. la responsable de entregar dicha clave pública a la CA de DOCUMENTA. S. A.

6.1.4 Entrega de la clave pública de la CA a los terceros 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)

6.1.5 Tamaño de las claves

El tamaño de las claves de los certificados de persona física es de 2048 bits.

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

La clave pública de los certificados de persona física emitidas por la CA de DOCUMENTA S. A está codificada de acuerdo con RFC 5280 y PKCS#1 siendo el algoritmo de generación de claves RSA.

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

Los usos admitidos de la clave para los certificados de persona física vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos.

El contenido de dichas extensiones para cada uno de los tipos de certificados de persona física se puede consultar en el apartado 7.1.2 del presente documento.

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

6.2.1 Estándares para los módulos criptográficos

Los dispositivos criptográficos con certificados de persona física, aptas como dispositivos seguros de creación de firma, contarán con la certificación FIPS 140-2 Nivel 2 o superior.

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

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

6.2.3 Custodia de la clave privada

La custodia de las claves privadas de los certificados de persona física la realizan los propios titulares de las mismas.

6.2.4 Copia de seguridad de la clave privada

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

6.2.5 Archivado de la clave privada

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

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

En ningún caso es posible transferir las claves privadas de firma de personas físicas para garantizar el no repudio.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas de firma de personas físicas se generan en el dispositivo criptográfico FIPS 140-2 nivel 2 o superior en el momento de la generación de los certificados.

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 Método de desactivación de la clave privada

No estipulado.

6.2.10 Método de destrucción de la clave privada

No La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del Módulo criptográfico de hardware la parte en la que estaba grabada la clave, para ello, éste debe ser limpiado por medio de inicialización de ceros (zeroize command).

6.2.11 Clasificación de los módulos criptográficos

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

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

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

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

El periodo de validez de los certificados de persona física 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

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

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 informática

6.5.1 Requerimientos técnicos específicos de seguridad informática

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

6.6 Controles de seguridad del ciclo de vida

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

6.6.1 Controles de desarrollo de sistemas

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.

6.7 Controles de seguridad de la red

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

6.8 Sellado de tiempo

Sin estipulaciones.

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 Perfil de certificado

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

A continuación se detalla el contenido de las extensiones más significativas de los certificados de persona física emitidos por la CA de DOCUMENTA S. A.

a) Certificado de persona física para Autenticación

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
G	JUAN ROLON
SN	ROMERO IMAS
SERIAL NUMBER	CI 9204032
CN	JUAN ROLON ROMERO IMAS (AUTENTICACION)
OU	PERSONA FISICA
O	JUAN ROLON ROMERO IMAS
C	PY

Descripción del resto de campos más relevantes del perfil de **certificado de persona física para autenticación**:

CAMPO	COMPONENTE PROPUESTO	CRITICA
1. Versión	V3	
2. Signature Algorithm	sha256WithRSAEncryption	
3. Issuer	CN = CA-DOCUMENTA S.A. O = DOCUMENTA S. A. C = PY SERIALNUMBER = RUC 80050172-1	
4. Validez	[PUEDE SER HASTA 2 AÑOS]	
5. Subject	G=[SE REGISTRA EL NOMBRE DEL TITULAR DEL CERTIFICADO, EN MAYÚSCULAS Y SIN TILDES. ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ" COMO UN CASO ESPECIAL PARA LOS NOMBRES DE PERSONAS FÍSICAS] SN=[SE REGISTRAN LOS DOS APELLIDOS DEL TITULAR DEL CERTIFICADO, EN MAYÚSCULAS Y SIN TILDES. ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ" COMO UN CASO ESPECIAL PARA APELLIDOS DE PERSONAS FÍSICAS] SERIAL NUMBER = [SIGLAS CI PARA CÉDULA DE IDENTIDAD DE PARAGUAYOS O SIGLAS CIE PARA CÉDULA DE IDENTIDAD DE EXTRANJEROS]espacio en blanco [NÚMERO DE IDENTIFICACIÓN PERSONAL] CN = [NOMBRE Y APELLIDO DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO DE IDENTIFICACIÓN, EN MAYÚSCULAS Y SIN TILDES ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ "COMO UN CASO ESPECIAL PARA NOMBRE Y APELLIDO DE PERSONA FÍSICA]espacio en blanco (AUTENTICACION) OU = PERSONA FISICA O = [NOMBRE Y APELLIDO DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO DE IDENTIFICACIÓN] C = [CÓDIGO DE PAÍS ES ASIGNADO DEACUERDO AL ISO 3166]	
6. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	
7. Certificate Policies **.Policy Identifier** **.URL CPS** **.Notice Referente**	**Se utilizará** https://www.documenta.com.py/firmadigital/descargas Este es un certificado de persona física para autenticación cuya clave privada está soportada por un dispositivo criptográfico seguro y cuyo único objeto es el de ser utilizado para autenticar a su titular.	**SI**
8. CRLDistributionPoints	https://www.documenta.com.py/firmadigital/descargas/crldoc.crl	NO

9. Auth. Information Access **.CAIssuers** **.OCSP**	**Se utilizará** **https://www.documenta.com.py/firmadigital/descargas/cadoc.crt** **http://www.documenta.com.py/firmadigital/oscp**	NO
10. KeyUsage	Firma Digital (Digital Signature) Cifrado de Clave (Key Encipherment)	**SI**
11. extKeyUsage	Autenticación del cliente Smart Card Logon	NO
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier **.KeyIdentifier** **.AuthorityCertIssuer** **.AuthorityCertSerialNumber**	**Se utilizará** SHA-1 hash de la clave pública del emisor **No utilizado** **No utilizado**	NO
14. qcStatements	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)[1]	NO

[1] **Indica que el certificado es compatible con la definición de certificado cualificado de IETF (*RFC 3739*).**

b) Certificado de persona física para Firma Digital

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
G	**JUAN ROLON**
SN	**ROMERO IMAS**
SERIAL NUMBER	**CI 9204032**
CN	**JUAN ROLON ROMERO IMAS (FIRMA)**
OU	**PERSONA FISICA**
O	**JUAN ROLON ROMERO IMAS**
C	**PY**

Descripción del resto de campos más relevantes del perfil de **certificado de persona física para firma digital**:

CAMPO	COMPONENTE PROPUESTO	CRITICA
1. Versión	V3	
2. Signature Algorithm	sha256WithRSAEncryption	
3. Issuer	CN = CA-DOCUMENTA S.A. O = DOCUMENTA S. A. C = PY SERIALNUMBER = RUC 80050172-1	
4. Validez	[PUEDE SER HASTA 2 AÑOS]	
5. Subject	G=[SE REGISTRA EL NOMBRE DEL TITULAR DEL CERTIFICADO, EN MAYÚSCULAS Y SIN TILDES. ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ" COMO UN CASO ESPECIAL PARA LOS NOMBRES DE PERSONAS FÍSICAS] SN=[SE REGISTRAN LOS DOS APELLIDOS DEL TITULAR DEL CERTIFICADO, EN MAYÚSCULAS Y SIN TILDES. ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ" COMO UN CASO ESPECIAL PARA APELLIDOS DE PERSONAS FÍSICAS] SERIAL NUMBER = [SIGLAS CI PARA CÉDULA DE IDENTIDAD DE PARAGUAYOS O SIGLAS CIE CÉDULA DE IDENTIDAD PARA EXTRANJEROS]espacio en blanco [NUMERO DE IDENTIFICACION PERSONAL] CN = [NOMBRE Y APELLIDO DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO DE IDENTIFICACIÓN, EN MAYÚSCULAS Y SIN TILDES. ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ "COMO UN CASO ESPECIAL PARA NOMBRE Y APELLIDO DE PERSONA FÍSICA]espacio en blanco (FIRMA) OU = PERSONA FISICA O = [NOMBRE Y APELLIDO DEL TITULAR DEL CERTIFICADO, SEGÚN DOCUMENTO DE IDENTIFICACIÓN.ÚNICAMENTE SE DEBE ACEPTAR EL CARÁCTER "Ñ" COMO UN CASO ESPECIAL PARA NOMBRE Y APELLIDO DE PERSONA FÍSICA] C = [CÓDIGO DE PAÍS ES ASIGNADO DEACUERDO AL ISO 3166]	
6. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: 2048 bits	
7. Certificate Policies **.Policy Identifier** **.URL CPS** **.Notice Referente**	**Se utilizará** https://www.documenta.com.py/firmadigital/descargas Este es un certificado de persona física para firma digital cuya clave privada está soportada por un dispositivo criptográfico seguro y cuyo único objeto es el de ser utilizado	**SI**

	para generar firmas digitales.	
8. CRLDistributionPoints	https://www.documenta.com.py/firmadigital/descargas/crldoc.crl	NO
9. Auth. Information Access **.CAIssuers** **.OCSP**	**Se utilizará** https://www.documenta.com.py/firmadigital/descargas/cadoc.crt http://www.documenta.com.py/firmadigital/oscp	NO
10. KeyUsage	No repudio (NonRepudiation)	**SI**
11. extKeyUsage	Protección del correo	NO
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier **.KeyIdentifier** **.AuthorityCertIssuer** **.AuthorityCertSerialNumber**	**Se utilizará** SHA-1 hash de la clave pública del emisor **No utilizado** **No utilizado**	NO
14. qcStatements	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)[1]	

[1] **Indica que el certificado es compatible con la definición de certificado cualificado de IETF (*RFC 3739*).**

7.1.3 Identificadores de objeto (OID) de los 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 Formatos de nombres

Los certificados emitidos por la CA de DOCUMENTA S. A. contienen el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

7.1.5 Restricciones de los nombres

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, 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 Notice Reference 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

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

7.2.1 Número de versión

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

7.2.2 CRL y extensiones

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.

7.4 Número(s) de versión

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

7.5 Extensiones OCSP

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

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia o circunstancias de los controles para cada Autoridad

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

8.2 Identificación/cualificación del auditor

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

8.3 Relación entre el auditor y la Autoridad auditada

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

8.4 Aspectos cubiertos por los controles

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

8.5 Acciones a tomar como resultado de la detección de deficiencias

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. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

Las tarifas correspondientes a la emisión o renovación de certificado se encuentran detalladas en la dirección https://www.documenta.com.py/firmadigital/tarifa

9.1.2 Tarifas de acceso a los 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 la información de 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 de otros servicios tales como información de políticas

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 Política de reembolso

Si al momento del cese de actividades por parte de la CA de DOCUMENTA S. A. el certificado de persona física para firma digital tiene una vigencia pendiente de uso superior a seis meses, DOCUMENTA S. A. deberá reembolsarle el importe de la tarifa proporcional a la vigencia no utilizada, a menos de que DOCUMENTA S. A. al cese en sus actividades haya transferido los certificados a otro prestador de servicios de certificación.

9.2 Responsabilidades económicas

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

9.2.1 Confidencialidad de la información

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

9.2.2 Ámbito de la información confidencial

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

9.2.3 Información no confidencial

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

9.2.4 Deber de secreto profesional

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

9.3 Protección de la información personal

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

9.3.1 Plan de Privacidad

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

9.3.2 Información tratada como privada

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

9.3.3 Información que no es considerada como privada

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

9.3.4 Responsabilidad para proteger información privada

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

9.3.5 Notificación y consentimiento para usar información privada

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

9.3.6 Divulgación de acuerdo con un proceso judicial o administrativo

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

9.3.7 Otras circunstancias de divulgación de información

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

9.4 Derechos de propiedad intelectual

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

9.5 Representaciones y garantías

9.5.1 Obligaciones de las CAs

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

9.5.2 Obligaciones de las RAs

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

9.5.3 Obligaciones de los titulares de los certificados

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

9.5.4 Obligaciones de los terceros que confían o acepten los certificados

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

9.6 Exención de responsabilidades

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

9.7 Limitaciones de las responsabilidades

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

9.8 Indemnizaciones

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

9.9 Período de validez

9.9.1 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.

9.9.2 Sustitución y derogación de la CP

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.

9.9.3 Efectos de la finalización

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.

9.10 Notificaciones individuales y comunicaciones con los participantes

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

9.11 Procedimientos de cambios en las especificaciones

9.11.1 Procedimiento para los cambios

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

9.11.2 Circunstancias en las que el OID debe ser cambiado

Sin estipulaciones.

9.12 Reclamaciones

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

9.13 Normativa aplicable

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

9.14 Cumplimiento de la normativa aplicable

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

9.15 Estipulaciones diversas

9.15.1 Cláusula de aceptación completa

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

9.15.2 Asignación

Sin estipulaciones.

9.15.3 Independencia/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.

9.15.4 Aplicación (Honorarios de Abogados y renuncia de derechos)

Sin estipulaciones.

9.15.5 Fuerza mayor

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

9.15.6 Resolución por la vía judicial

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

9.16 Otras estipulaciones

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.