DECLARACIÓN DE PRÁCTICAS CERTIFICACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ

Ministerio de Industria y Comercio
Viceministerio de Comercio
República del Paraguay

DOC-PKI-01
VERSION 4.0

CONTROL DOCUMENTAL

Documento	
Título: Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.	**Nombre Archivo:**
Código: DOC-PKI-01	**Soporte Lógico:**
Fecha: 31/10/2016	**Ubicación Física:** DGFDyCE
Versión: 4.0	

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Autoridad Certificadora (CA)	Prestadores de Servicio de Certificación (PSC)
Documento Público	www.acraiz.gov.py

Control del Documento		
Preparado por:	**Revisado por:**	**Aceptado por:**
Ing. Lucas Sotomayor ***Lic. Claudia Dacak*** ***M. Sc. Mario Monges***	***MSc. Jenny Ruíz Díaz***	***M. Sc. Rodys Rolón***

Tabla de contenido

1. INTRODUCCIÓN

1.1. Descripción general

El Ministerio de Industria y Comercio (MIC), a través del Viceministerio de Comercio, se constituye en la Autoridad de Aplicación (AA) conforme lo dispone la Ley que rige la materia. La Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE) es la dependencia designada para ejecutar las funciones atribuidas al MIC en su calidad de AA.

Entre sus funciones principales se encuentran:

- Administrar la Autoridad Certificadora Raíz del Paraguay (CA Raíz).
- Dictar las normas que regulen los servicios de certificación digital en el país.
- Recepcionar, procesar y expedirse sobre solicitudes de habilitación de interesados en constituirse en Prestadores de Servicios de Certificación (PSC).
- Inspeccionar y auditar al Prestador de Servicios de Certificación habilitado.
- Revocar la habilitación del PSC.
- Imponer sanciones al PSC.

En la cúspide de la jerarquía de la Infraestructura de Clave Pública del Paraguay (PKI Paraguay), por sus siglas en inglés Public Key Infrastructure se ubica la CA Raíz, la misma cuenta con un certificado autofirmado y aceptado por los terceros que confían en la PKI Paraguay.

Los certificados digitales emitidos por la CA Raíz se rigen y ajustan a la presente Declaración de Prácticas de Certificación (CPS) y la correspondiente Política de

Certificación (CP), cuyo cumplimiento es de carácter obligatorio.

Esta CPS fue elaborada conforme a las recomendaciones establecidas en el RFC 3647 ‘’INTERNET X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework’’; y contiene los principios y reglas relativos a la gestión de certificados digitales, las normas mínimas y básicas que debe cumplir la CA Raíz, el uso de los certificados digitales, entre otras cuestiones relacionadas con la PKI Paraguay.

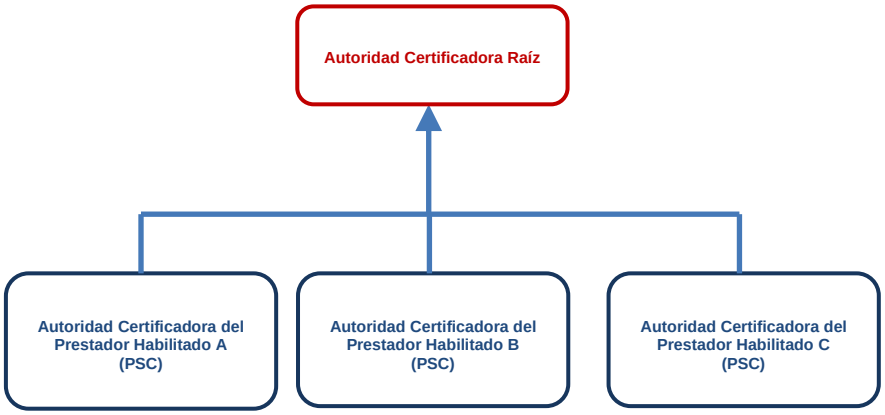
En resumen, esta CPS es específicamente aplicable a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz)
- Prestador de Servicios de Certificación (PSC)
    - Autoridad de Certificación Intermedia
    - Autoridad de Registro (RA)
    - Autoridad de Validación (VA)
- Suscriptor
- Parte que confía

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 como se muestra en la figura 1.

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.

Figura 1



1.2 Nombre e Identificación del documento

Nombre: Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz del Paraguay.

Versión: 4.0

Fecha de aprobación: _____

Sitio de Internet oficial: http://www.acraiz.gov.py/cps/politicas.pdf

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras (CA)

- Ministerio de Industria y Comercio (MIC), en su carácter de Autoridad Certificadora Raíz del Paraguay (CA Raíz) o Autoridad de Certificación Raíz del Paraguay (CA Raíz), indistintamente; emite certificados a los PSC bajo la jerarquía del Certificado Raíz, el cual es auto-firmado, y a partir de él se inicia la cadena de confianza. Subordinados al certificado raíz, se encuentran

los certificados emitidos al PSC.

- Prestador de Servicios de Certificación (PSC), en su carácter de Autoridad Certificadora Intermedia, es la persona jurídica que emite certificados digitales para personas físicas y/o jurídicas que permiten identificar a dichos titulares. 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. Autoridad de Registro (RA)

La RA ejecuta labores de identificación y autenticación del solicitante de un certificado. La misma, debe validar los requisitos de identificación del solicitante, dependiendo del tipo de certificado y de la especificación de la política pertinente. Además, tramita las solicitudes de emisión y revocación de certificados. La DGFDyCE y el PSC cumplen funciones de RA.

La actividad de identificación y registro del PSC será realizada durante el proceso de habilitación, no habiendo otra autoridad de registro en el ámbito de la CA Raíz, más que la DGFDyCE.

El PSC podrá delegar las funciones de registro a otras organizaciones, que siempre estarán bajo su responsabilidad y control, cumpliendo las normas y procedimientos establecidos en la normativa vigente, previa comunicación y autorización de la AA.

La RA podrá llevar a cabo sus actividades en una sede fija o en modalidad móvil, siempre que medie autorización de la AA.

La RA se encarga de garantizar y cumplir con las siguientes tareas:

- que los documentos aportados para la identificación y acreditación de la capacidad de representación, sean auténticos y suficientes para llevar a cabo este trámite;
- en la medida de sus posibilidades, corroborar que el solicitante y cuantas personas intervengan en el trámite de solicitud, sean capaces, y lo realicen libre y voluntariamente;
- que las consultas y dudas que les sean formuladas, sean atendidas;
- poner a disposición del solicitante y de todas las personas que intervienen en el trámite de solicitud, la CPS, CP, tasas y aranceles del servicio, así como toda información relacionada con el proceso de emisión y de revocación: causas, obligaciones y procedimiento a seguir;
- informar a los solicitantes, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso;
- verificar que el titular de los datos ha prestado su consentimiento para el tratamiento de sus datos personales, en conocimiento de la finalidad que se les va a dar; y
- procesar toda la documentación presentada por el solicitante y enviar la solicitud de certificado a la CA de forma segura y firmada digitalmente.

El responsable del Registro que realiza el trámite deberá archivar todas las documentaciones referentes al proceso de registro y firmarlo digitalmente.

Deberá hacer entrega del certificado solicitado y el Acuerdo de Suscriptores firmado por las partes.

1.3.3. Suscriptores

Respecto a la CA Raíz, es suscriptor el PSC; en relación a este último, es suscriptor toda persona física o jurídica a quien se emite un certificado digital, dentro

de la jerarquía PKI Paraguay.

1.3.4. 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 dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.5. Otros participantes

Sin estipulaciones.

1.4. Uso del Certificado

1.4.1 Usos apropiados del Certificado

Las CP de la CA Raíz y del PSC, correspondientes a cada tipo de certificado que emita, son las que determinan los usos apropiados que deben darse a cada certificado.

1.4.2. Usos prohibidos del certificado

En cada CP se determina las limitaciones y restricciones en el uso de los certificados. No es objetivo de esta CPS la determinación de dichas limitaciones y restricciones.

1.5 Administración de la Política

1.5.1. Organización que administra el documento

Nombre: Ministerio de Industria y Comercio (MIC).

Dirección: Avenida Mcal. López 3333. Asunción, Paraguay.

Teléfono: (+595) (21) 616-3000.

Dirección de correo electrónico: consultas@mic.gov.py

Página Web: www.mic.gov.py

1.5.2. Persona de Contacto

Nombre: Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE).

Dirección: Capitán Pedro Villamayor Teófilo, esquina Capitán Nicolás Blinoff. Asunción, Paraguay.

Teléfono: (+595) (21) 616-3000.

Dirección de correo electrónico: info-dgfdce@mic.gov.py

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

En el caso de la CPS de la CA Raíz, la máxima autoridad institucional, será la encargada de determinar la adecuación de la Declaración de Prácticas de Certificación (CPS) de la CA Raíz.

El PSC deberá designar ante la AA, el responsable competente para determinar la adecuación de su CPS a la CP que implemente según la normativa vigente.

1.5.4 Procedimientos de aprobación de la Declaración de Prácticas de Certificación (CPS)

El MIC aprobará el contenido de la presente CPS y sus posteriores enmiendas o modificaciones, por resolución ministerial. Se podrá someter consideración de entidades públicas y privadas relacionadas al área, para que emitan sus comentarios y sugerencias, previo al trámite de aprobación. El PSC deberá establecer sus procedimientos para aprobación y puesta en vigencia de su CPS y ser aprobadas por la AA.

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, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita de las partes intervinientes.

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 ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.

Autoridad de Aplicación (AA): se designa al 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 por Ley, establecido por el artículo 38 de la Ley Nº 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 de Certificación (CA): entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI Paraguay, son Autoridades de Certificación, la CA Raíz del Paraguay y el PSC.

Autoridad Certificadora Raíz o Autoridad de Certificación Raíz (CA Raíz): es el órgano técnico dentro PKI, cuya función principal es habilitar al PSC y emitir a este, su certificado digital correspondiente. Posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza.

Autoridad Certificadora Intermedia: entidad cuyo certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz, es responsable de la emisión de certificados al usuario final.

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 interviene 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 digitales 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 relacionadas.

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 aberturas 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 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 al par de 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 del certificado, 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 PSC 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 los 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, que 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): Los identificadores de objeto son un sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las recomendaciones UIT-T y las normas internacionales ISO.

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 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 criptosistema 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 el 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

Acrónimo	Descripción
C	País (por su siglas en inglés, country)
CA	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
CAI	Autoridad de Certificación Intermedia (CA por sus siglas en inglés, Certificate Authority Intermediate)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de Identidad
CN	Nombre Común (por sus siglas en inglés, Common Name)
CP	Política 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)
CWA	Documento de Referencia del Comité Europeo de Normalización (CEN) desarrollado y aprobado en un taller de trabajo, algunos de los CWA son específicos para firma electrónica (CEN Workshop Agreement)
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio.
DNS	Sistema de Nombre de Dominio (DNS por sus siglas en inglés, Domain Name System).
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	Módulo de seguridad criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization)

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 (por sus sigla en inglés, Organization)
OCSP	Servicio de Validación de Certificados en Línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU, por sus siglas en inglés, Organization Unit)
PIN	Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number)
PKCS	Normas 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 (por sus siglas en inglés, Serial Number)
TLS	Capa de conexión 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 pos sus siglas en inglés, Validation Authority)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1. Repositorios

La CA Raíz dispone del siguiente sitio de Internet como repositorio público de información: https://www.acraiz.gov.py y cuyo acceso será gratuito e irrestricto.

2.2 Publicación de Información de Certificación

Es obligación de la CA pertenecientes a la jerarquía de confianza de la PKI Paraguay, publicar la información relativa a sus prácticas, sus certificados y el estado actual de dichos certificados.

La CA Raíz mantiene un repositorio en su sitio principal de Internet que permite a las partes que confían, verificar en línea la revocación de un certificado y cualquier otra información necesaria para validar el estado del mismo.

Mantiene publicada, entre otros aspectos la versión actualizada de:

- CP y CPS que implementa;
- El certificado de la CA Raíz;
- La lista de certificados revocados;
- Las Resoluciones de habilitación, suspensión o revocación del PSC;
- La información relevante de la última auditoría que hubiere sido objeto;
- Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay; y
- Identificación, domicilio y medios de contacto.

La CA Raíz dispone del siguiente sitio de Internet como repositorio público de información: https://www.acraiz.gov.py y cuyo acceso será irrestricto.

El servicio de publicación de información de una CA Raíz deberá estar disponible durante las veinticuatro horas, los siete días de la semana. En caso de interrupción

por causa de fuerza mayor, el servicio se restablecerá en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

La CA Raíz dedicará sus mejores esfuerzos para que el servicio se restablezca y esté disponible rápidamente.

2.3 Tiempo o frecuencia de Publicación

La información de estados de certificado, es publicada conforme lo dispuesto en el punto 4.9.7 de esta CPS.

Las demás informaciones mencionadas en el punto 2.2, serán actualizadas lo más pronto posible y con un máximo de un día hábil desde que se dispongan o surjan modificaciones.

2.4 Controles de Acceso a los Repositorios

La información publicada en el repositorio, es información accesible únicamente para consulta. La CA debe establecer controles para prevenir que personas no autorizadas agreguen, eliminen o modifiquen información de su repositorio.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

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.

El procedimiento de asignación de los nombres distintivos a los suscriptores para cada uno de los tipos de certificados se encuentra definido en la CP. Dicha definición debe estar en consonancia con las directrices generales descritas en este capítulo de la CPS.

3.1.2. Necesidad de Nombres significativos

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 la PKI Paraguay para interpretar los nombres distintivos de los titulares de certificados que emite, es ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 Unicidad de los Nombres

El conjunto de nombre distintivo (Distinguished Name) más el contenido de la extensión Policy Identifier debe ser único y no ambiguo.

Los procedimientos de garantía de la unicidad para cada tipo de certificado están establecidos en la CP.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

La CA Raíz no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas o instituciones y marcas registradas**.** La CA Raíz tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

3.2 Validación inicial de identidad

3.2.1 Método para probar posesión de la clave privada

El solicitante del certificado debe demostrar que posee la clave privada correspondiente a la clave pública que deberá ser listada en el Certificado. La posesión de la clave privada, correspondiente a la clave pública para la que se solicita que se genere el certificado, quedará probada mediante el envío de la solicitud de firma de certificado (CSR) en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por la DGFDyCE, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 Autenticación de identidad de Persona Jurídica

Conforme lo estipulado en la CP.

3.2.3 Autenticación de identidad de Persona Física

No aplica

3.2.4 Información del Suscriptor no verificada

No aplica.

3.2.5. Validación de la Autoridad (Capacidad de hecho)

Conforme lo estipulado en la CP.

3.2.6. Criterios para operar con CA externas a la PKI Paraguay

La CA Raíz podrá suscribir acuerdos de reconocimientos mutuos con entidades similares, a fin de reconocer la validez de certificados digitales otorgados en el extranjeros. La CA externa ha de proporcionar un nivel de seguridad en la gestión de los certificados, a lo largo de su ciclo de vida, como mínimo, igual al de la PKI Paraguay.

3.3 Identificación y autenticación para solicitudes de re emisión de claves

3.3.1 Identificación y autenticación para re emisión de claves rutinaria

Conforme lo estipulado en la CP.

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

Conforme lo estipulado en la CP.

3.4 Identificación y autenticación para solicitudes de revocación

Conforme lo estipulado en la CP.

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 Solicitud del Certificado

4.1.1 Quién puede presentar una solicitud de certificado

Conforme a lo estipulado en la CP.

4.1.2 Proceso de Inscripción y responsabilidades

Conforme a lo estipulado en la CP.

4.2. Procesamiento de la Solicitud del Certificado

4.2.1 Ejecución de las funciones de Identificación y Autenticación

Conforme a lo estipulado en la CP.

4.2.2 Aprobación o rechazo de solicitudes de certificado

Conforme a lo estipulado en la CP.

4.2.3. Tiempo para procesar solicitudes de Certificado

Conforme a lo estipulado en la CP.

4.3 Emisión del Certificado

4.3.1 Acciones de la CA durante la emisión de los certificados

Conforme a lo estipulado en la CP.

4.3.2 Notificación al suscriptor sobre la emisión del Certificado Digital

Conforme a lo estipulado en la CP.

4.4. Aceptación del Certificado

4.4.1 Conducta constitutiva de aceptación de certificado

Conforme a lo estipulado en la CP.

4.4.2 Publicación del Certificado por la CA

Conforme a lo estipulado en la CP.

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

Conforme a lo estipulado en la CP.

4.5 Uso del par de claves y del certificado

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

Conforme a lo estipulado en la CP.

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

Conforme a lo estipulado en la CP.

4.6 Renovación del certificado

Conforme a lo estipulado en la CP.

4.6.1 Circunstancias para renovación de certificado

Conforme a lo estipulado en la CP.

4.6.2 Quién puede solicitar renovación

Conforme a lo estipulado en la CP.

4.6.3 Procesamiento de solicitudes de renovación de certificado

Conforme a lo estipulado en la CP.

4.6.4 Notificación al suscriptor sobre la emisión de un nuevo certificado

Conforme a lo estipulado en la CP.

4.6.5 Conducta constitutiva de aceptación de un certificado renovado

Conforme a lo estipulado en la CP.

4.6.6 Publicación por la CA del certificado renovado

Conforme a lo estipulado en la CP.

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

Conforme a lo estipulado en la CP.

4.7 Renovación del certificado sin cambio de clave

Conforme a lo estipulado en la CP.

4.7.1 Circunstancias para re-emisión de claves de certificado

No aplica.

4.7.2 Quien puede solicitar la certificación de una clave pública

No aplica.

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

No aplica.

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

No aplica.

4.7.5 Conducta constitutiva de aceptación de un certificado re-emitido

No aplica.

4.7.6 Publicación por la CA de los certificados re-emitidos

No aplica.

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

No aplica.

4.8 Modificación de certificados

4.8.1 Circunstancias para modificación del certificado

No aplica.

4.8.2 Quién puede solicitar modificación del certificado

No aplica.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.8.5 Conducta constitutiva de aceptación del certificado modificado

No aplica.

4.8.6 Publicación por la CA de los Certificados modificados

No aplica.

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

No aplica.

4.9 Revocación y suspensión

4.9.1 Circunstancias para la revocación

Conforme a lo estipulado en la CP.

4.9.2 Quien puede solicitar Revocación

Conforme a lo estipulado en la CP.

4.9.3 Procedimiento para la solicitud de revocación

Conforme a lo estipulado en la CP.

4.9.4 Periodo de gracia para solicitud de revocación

Conforme a lo estipulado en la CP.

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

Conforme a lo estipulado en la CP.

4.9.6 Requerimientos de verificación de revocación para las partes que confían

Conforme a lo estipulado en la CP.

4.9.7 Frecuencia de Emisión del CRL

Conforme a lo estipulado en la CP.

4.9.8 Latencia máxima para CRL

Conforme a lo estipulado en la CP.

4.9.9 Disponibilidad de verificación de revocación/ estado en línea

Conforme a lo estipulado en la CP.

4.9.10 Requerimientos para verificar la revocación en línea

Conforme a lo estipulado en la CP.

4.9.11 Otras formas de advertencias de revocación disponibles

Sin estipulaciones

4.9.12 Requerimientos especiales por compromiso de clave privada

Conforme a lo estipulado en la CP.

4.9.13 Circunstancias para suspensión

No aplica.

4.9.14 Quien puede solicitar la suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del período de suspensión

No aplica.

4.10 Servicios de comprobación de estado de Certificado

4.10.1 Características operacionales

Conforme a lo estipulado en la CP.

4.10.2 Disponibilidad del Servicio

Conforme a lo estipulado en la CP.

4.10.3 Características opcionales

Sin estipulaciones

4.11 Fin de la suscripción

Conforme a lo estipulado en la CP.

4.12 Custodia y recuperación de claves

4.12.1 Política y prácticas de custodia y recuperación de claves

Conforme a lo estipulado en la CP.

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

No aplica.

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

La CA mantiene controles de seguridad no técnicos (esto es, controles físicos, procedimientos y de personal) para asegurar la ejecución de las funciones de generación de clave, autenticación de los sujetos, emisión del certificado, revocación del certificado, auditoría y almacenamiento.

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

Las operaciones de la CA, deben estar dentro de un ambiente de protección física que impida y prevenga usos o accesos no autorizados o divulgación de información sensible.

Las instalaciones de la CA deberán contar con los siguientes perímetros de seguridad física:

- primer perímetro: acceso a las instalaciones de la CA. Área de recepción;
- segundo perímetro: acceso al área de procesos administrativos de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el primero;
- tercer perímetro: acceso al área de operación de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo;
- cuarto perímetro: acceso al área de operaciones críticas de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el tercero;
- quinto perímetro: acceso al área de resguardo de documentos y dispositivos sensibles. Área interna al cuarto perímetro; y
- sexto perímetro: acceso al área de resguardo de clave privada. Área interna al cuarto perímetro.

El edificio que contiene las unidades de procesamiento de información debe ser físicamente sólido, los muros externos deben ser de construcción sólida, dotados de niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Todas las puertas y ventanas deben estar cerradas y protegidas contra accesos no autorizados. Las aberturas deben ser de estructura sólida y dotada de un sistema de cierre seguro y resistente.

La generación de claves y emisión de los certificados de la CA se deben realizar en un centro de datos (Data center) situado en una infraestructura de alta seguridad conforme los perímetros de seguridad señalados.

Las instalaciones donde se crean los certificados de la CA, se debe proteger con su propio y único perímetro físico, y las barreras físicas (paredes y barrotes) son sólidas, extendiéndose desde el piso real al cielo raso real.

Los sistemas deben estar físicamente separados de otros existentes en el lugar, de forma que solo el personal autorizado de la CA puede acceder a ellos, garantizando así la independencia de otros equipos.

Las instalaciones deberán contar con las siguientes medidas de protección:

- servicio de vigilancia las 24 horas;
- ambiente alejado de sótanos para prevenir posibles inundaciones;
- el edificio debe estar situado en un sitio de fácil y rápido acceso en caso de necesidad, por parte de los servicios de orden público y bomberos;
- el edificio se debe encontrar en una zona sin antecedentes de catástrofes naturales y de baja actividad sísmica;
- el edificio debe situarse en zona de bajo nivel de delincuencia;
- sistema de energía y aire acondicionado redundantes;

- mecanismos de prevención destinados a reducir el efecto del contacto con el agua;
- mecanismos de prevención y protección contra incendios; y
- todo el cableado deberá estar protegido contra daños o interceptación electromagnética, o interceptación de la transmisión tanto de datos como de telefonía.

5.1.2 Acceso físico

Los controles de acceso físico deben evitar el ingreso no autorizado a las instalaciones de la CA.

Para acceder al primer perímetro de seguridad se requerirá que todo individuo sea identificado por el personal autorizado. En este perímetro no se realizará ninguna operación ni proceso administrativo de la CA.

Para acceder al segundo perímetro de seguridad se requerirá como mínimo un factor de autenticación y tarjeta de identificación visible. En este perímetro, se desarrollan procesos administrativos de la CA.

Para acceder al tercer perímetro de seguridad se requerirá como mínimo 2 factores (contraseña y tarjeta de proximidad). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por, al menos un personal de la CA. En ésta área se desarrollan actividades como: servicios de soporte, climatización, energía, comunicaciones, monitoreo, validación de CSR, publicación en el repositorio, entre otras.

Para acceder al cuarto perímetro de seguridad se requerirá como mínimo 2 factores de autenticación (al menos uno de ellos debe ser biométrico). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por, al menos dos personales de la CA. En ésta área se realizan actividades de emisión y revocación de certificados, emisión de CRL.

El quinto perímetro de seguridad, constituye un recinto acorazado (cofre de seguridad), el acceso al mismo solo es permitido al personal autorizado. En ésta área se almacenan documentos y dispositivos sensibles inherentes a la operativa de la CA.

El sexto perímetro de seguridad, constituye un gabinete reforzado con cerraduras antirrobo (rack cofre), el acceso al mismo solo es permitido al personal autorizado. En ésta área se almacena la clave privada de la CA.

Cuando las instalaciones operacionales de la CA estén desocupadas, deben estar cerradas con clave y con las alarmas debidamente activadas.

Los perímetros deben ser auditados y controlados para verificar que solo puede tener acceso el personal autorizado debidamente identificado.

Los derechos de acceso a las instalaciones de la CA deben revisarse y actualizarse regularmente, al menos cada seis meses o cuando se presente movimiento del personal relacionado con labores de operación de la CA.

Los terceros que requieran acceso a las instalaciones operacionales de la CA, deben ser escoltados y registrarse ante el responsable de autorizar el acceso, la fecha y hora de entrada y salida.

5.1.3 Energía y Aire acondicionado

Las áreas donde se ubican los equipos de la infraestructura tecnológica de la CA, deben contar con suministros de electricidad y aire acondicionados adecuados a los requisitos de los equipos en ellas instalados. La infraestructura debe encontrarse protegida contra caídas de tensión o cualquier otra anomalía en el suministro eléctrico. Las instalaciones deben disponer de:

1. Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés Uninterruptible Power Supply).

2. Grupo electrógeno con potencia suficiente para soportar la carga del centro de datos (Data Center), incluido los equipos informáticos y equipos de refrigeración.

Las instalaciones deben estar equipadas con sistemas de energía primario y de respaldo para asegurar continuidad del fluido eléctrico.

Las instalaciones deben contar con sistemas de aire acondicionado de precisión redundantes. El equipo instalado para climatizar el recinto, debe ser capaz de controlar la humedad relativa del mismo.

5.1.4 Exposiciones al agua

Las instalaciones de la CA deben ser construidas y equipadas para prevenir inundaciones y otros daños por exposición al agua y deberán ser implementados procedimientos a tal efecto.

Deben estar protegidas para evitar exposiciones al agua, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

5.1.5 Prevención y protección contra fuego

El área donde se encuentra la infraestructura tecnológica de la CA debe disponer de sistemas inteligentes de detección y extinción de incendios para la protección de su contenido. El cableado debe situarse en un falso suelo o techo y deben disponer de los medios adecuados (detectores en suelo y techo) para la protección del mismo contra incendios.

Las instalaciones de la CA deberán ser construidas y equipadas para prevenir, detectar y suprimir incendios o daños producidos por la exposición a llamas o humo, y contar con procedimientos implementados para la prevención y protección al fuego.

5.1.6 Almacenamiento de medios

La información relacionada a la infraestructura de la CA debe almacenarse de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida. Los cofres de seguridad deben ser de acero o material de resistencia equivalente, debe ofrecer tolerancia:

- Al fuego por al menos 60 minutos; y
- Aberturas forzadas.

Asimismo, debe poseer tranca con llave manual o electrónica. Debe ser suficientemente pesado, de forma a dificultar su retiro o deberá ser fijado al piso.

La CA debe asegurar el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y debe impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

5.1.7 Eliminación de residuos

La CA debe implementar controles para la eliminación de residuos (papel, medios, equipos y cualquier otro desecho), con el fin de prevenir el uso no autorizado, el acceso o divulgación de información privada y confidencial contenida en los desechos.

Los documentos y materiales sensibles deben ser triturados antes de su eliminación. Los medios utilizados para capturar o transmitir información sensible deben ser dejados ilegibles antes de su eliminación. Los dispositivos criptográficos deben ser destruidos físicamente o su contenido dejado en cero de acuerdo a la guía del fabricante antes de su eliminación.

Otros desechos deberán ser eliminados de acuerdo a los requerimientos de eliminación de desechos normales definidos por la CA.

5.1.8 Respaldo fuera de sitio

La CA debe contar con una instalación alterna, con niveles de protección física y ambiental similar al sitio principal y con una separación física adecuada.

La CA debe mantener respaldo de los datos críticos del sistema y de cualquier otra información sensible, incluyendo los datos de auditoría, en una instalación segura fuera del sitio principal.

Las copias de seguridad externa deben ser establecidas y mantenidas de conformidad con la política de continuidad del negocio y el plan de recuperación frente a desastres de manera compatible con los estándares internacionales.

5.2 Controles procedimentales

5.2.1 Roles de Confianza

La CA deberá garantizar la segregación de tareas para las funciones críticas, con el fin de evitar que un empleado que asume un rol de confianza utilice incorrectamente su sistema de certificación sin ser detectado. Las acciones de cada uno de los empleados se limitarán de acuerdo a su perfil.

Todos los operadores del sistema de certificación de la CA, deberán recibir entrenamiento específico antes de obtener cualquier tipo de acceso. El tipo o nivel de acceso serán determinados, en un documento formal, con base en las necesidades de cada perfil.

Cuando un empleado se desvincula de la CA, sus permisos de acceso deberán ser revocados inmediatamente. Cuando hay un cambio en la posición o función que el empleado ocupa dentro de la CA, deberán ser revisados sus permisos de acceso. Deberá existir una lista de revocación, con todos los recursos, antes

disponibilizados, que el empleado deberá devolver a la CA en el momento de su desvinculación

Los Roles de una CA, deben contemplar, al menos las siguientes responsabilidades que a continuación serán descriptos:

a) **Responsables de seguridad:** deberán llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobadas por la CA, controlar la formalización de los convenios entre el personal y la CA, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, deberá cumplir y hacer cumplir las políticas de seguridad de la CA y deberá encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Será el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls. Deberá comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a estos, asimismo deberá resolver o hacer que resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. y es el encargado de la gestión y control de la seguridad física, y de los movimientos de material fuera de las instalaciones de la CA;
b) **Responsables de coordinación de área:** es el responsable de autorizar tecnológicamente la emisión de un certificado o la revocación del mismo. Bajo su control y supervisión, se encuentra el personal adscripto a la misma. Es su responsabilidad: recibir y dar curso a las denuncias que podrían afectar a su personal, proponiendo las medidas disciplinarias correspondientes; efectuar un control permanente de la adecuación de los recursos materiales y

humanos que cuenta el área a su cargo, con el fin de atender las necesidades de servicio que tiene encomendadas;

c) **Responsables de sistemas:** los responsables de este rol no deberán estar implicados en tareas de auditoría interna. Serán encargados de la instalación y configuración de sistemas operativos, del mantenimiento y actualización de los programas instalados; con capacidad para configurar y mantener los sistemas, pero sin acceso a los datos. Asimismo, deberán establecer y documentar los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Serán responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación de la CA y asumirán la gestión de los servicios de ruteo y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Serán encargados de la instalación de hardware criptográfico de la CA y de la eliminación del hardware criptográfico de la CA de producción. Serán responsables del mantenimiento o reparación de equipos criptográficos de la CA (incluida la instalación de nuevo hardware, firmware o software), y la eliminación de desmontaje y permanente por el uso;

d) **Responsables de la operación diaria de la CA**: serán los encargados de realizar las tareas de ejecución y revisión de las copias de seguridad del sistema. Asimismo debe velar para que se lleven a cabo las copias de seguridad local y del traslado de las mismas de acuerdo con lo establecido en la política de seguridad. Serán responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Serán encargados de la gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios;

e) **Responsables de auditoría interna:** serán los responsables de las tareas de ejecución y revisión de auditoría interna del sistema. Esta auditoría interna se deberá realizar conforme con las normas y criterios de auditoría

establecidos en la presente CPS y la normativa vigente. Además deberá tener acceso a todos los registros del sistema;

f) **Responsables del ciclo de vida de claves criptográficas:** se distinguen los siguientes responsables para la gestión del ciclo de vida de las claves criptográficas:
   I. **Oficial criptográfico:** será el responsable de generar los usuarios que van a hacer uso de las claves del HSM. Participa en la copia de respaldo y recuperación del HSM;
   II. **Oficial de activación:** será el responsable de activar las claves del HSM para que se pueda hacer uso de las mismas;
   III. **Usuario:** serán quienes operan el sistema de gestión de certificados y el HSM;
   IV. **Oficial de registro:** realizará funciones de registro, como la generación de certificados o la revocación de los mismos; y
   V. **Oficial de generación de CRL:** Encargado de generar y exportar en ficheros, los CRL emitidas por el PSC. Además son responsables de activar los servicios de OCSP y asegurar la disponibilidad del CRL.

g) **Responsables de desarrollo de sistemas de la CA:** serán los encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones.

5.2.2 Número de personas requeridas por tarea

La CA debe establecer, mantener y ejecutar procedimientos de control rigurosos para asegurar la segregación de funciones, basados en las responsabilidades del trabajo y la cantidad de personas de confianza que ejecutan las tareas sensibles (como mínimo dos personas).

5.2.3 Identificación y autenticación para cada rol

Para toda persona que aspira asumir un rol de confianza, la verificación de identidad es realizada a través de la presencia física ante personal autorizado de la CA y una revisión de formas de identificación comúnmente reconocidas (cédula de identidad, pasaporte). La identidad es confirmada adicionalmente a través de los procedimientos de comprobación de antecedentes establecidos en el punto 5.3.1 de la presente CPS.

La CA debe asegurarse de que el personal ha alcanzado el estado de confianza antes de que a la persona aspirante:

- Le sean emitidos dispositivos de acceso y concedido acceso a las instalaciones requeridas; y
- Le sean emitidas credenciales electrónicas para acceder y realizar funciones específicas en la CA u otros sistemas de la infraestructura tecnológica.

.

5.2.4 Roles que requieren separación de funciones

En este ítem la CPS describirá aquellos roles que requieren separación de funciones. Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

- Los responsables del ciclo de vida de claves criptográficas no podrán cumplir funciones de los responsables de auditoría interna;
- Los responsables de sistemas no podrán cumplir funciones de los responsables de seguridad, ni de los responsables de auditoría interna;

- Los responsables de seguridad no podrán cumplir funciones de los responsables de sistemas, de los responsables del ciclo de vida de claves criptográficas, ni de los responsables de auditoría interna; y
- los responsables de auditoría no podrán cumplir otra función o rol.

Además otras tareas que deben ser segregadas son:

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

5.3 Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y autorización

Las CA deben suscribir un documento con las personas designadas para desempeñar roles de confianza en el que se establecerá las funciones, obligaciones, responsabilidades y sanciones. Las personas designadas, además deben:

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

Todo el personal que preste sus servicios en el ámbito de la PKI deberá poseer el conocimiento, experiencia y formación suficientes para el mejor cometido de las funciones asignadas. Para ello se llevarán a cabo los procesos de selección de personal que la CA estime precisos con objeto de que el perfil profesional se adecue lo más posible a las características propias de las tareas a desarrollar.

5.3.2 Procedimientos de verificación de antecedentes

La CA debe contar con procedimientos para verificar la experiencia y los antecedentes del personal propuesto para un rol de confianza. Algunos aspectos de la investigación de antecedentes incluyen:

- confirmación de empleos anteriores;
- verificación de referencias profesionales;
- título académico obtenido; y
- verificación de antecedentes judiciales y policiales.

5.3.3 Requerimientos de capacitación

Todo el personal involucrado en las operaciones de la CA debe estar capacitado apropiadamente, en aspectos tales como:

- operación del software y hardware;
- políticas y procedimientos organizacionales;
- procedimientos de seguridad y operacionales; y
- normativa vigente que rige la materia.

Todo personal recibirá la formación necesaria para asegurar la correcta realización de sus funciones tales como:

- Concienciación sobre la seguridad física, lógica y técnica;
- Procedimientos de operación y administración para cada rol específico; y

- Procedimientos para la recuperación de la operación de la CA en caso de desastres.

5.3.4 Requerimientos y frecuencia de capacitación

La CA debe capacitar al personal cuando se presenten cambios significativos en las operaciones de la CA, por ejemplo cuando se producen actualizaciones de hardware o software, cambios en los sistemas de seguridad, etc.

La CA debe proveer los programas de entrenamiento y actualización a su personal para asegurar que el mismo mantenga el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

La CA debe efectuar una rotación de sus roles de confianza. La frecuencia de la rotación del personal debe ser al menos una vez cada cinco años, para la CA Raíz.

Antes de asumir las nuevas labores, el personal debe recibir una nueva capacitación que le permita ejecutar las tareas satisfactoriamente.

5.3.6 Sanciones para acciones no autorizadas

La CA debe aplicar sanciones administrativas y disciplinarias al personal que violente las normas de seguridad establecidas en la CP o su CPS, de acuerdo a lo estipulado en el documento suscripto para los roles de confianza.

5.3.7 Requisitos de contratación a terceros

La CA puede contratar personal externo o consultores bajo las siguientes condiciones:

- existe un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas;
- no se posee personal disponible para llenar los roles de confianza;

- los mismos cumplen con los mismos requisitos del punto 5.3.1;
- una vez finalizado el servicio contratado se revocan los derechos de acceso; y
- deben firmar un acuerdo de confidencialidad como parte de los términos y condiciones de su incorporación.

5.3.8 Documentación suministrada al personal

La CA debe suministrar suficiente documentación al personal para que ejecute un rol, donde se definen los deberes y procedimientos para el correcto desempeño de su función.

5.4 Procedimiento de Registro de auditoría

La CA debe mantener controles para proveer una seguridad razonable de que:

- los eventos relacionados con el ambiente de operación de la CA, la gestión de las claves y los certificados, son registrados exacta y apropiadamente;
- se mantiene la confidencialidad y la integridad de los registros de auditoría vigentes y archivados;
- los registros de auditoría son archivados completa y confidencialmente; y
- los registros de auditoría son revisados periódicamente por personal autorizado.

5.4.1 Tipos de eventos registrados

La CA debe registrar los tipos de eventos que se presentan en sus operaciones. La CA debe mantener los registros manuales o automáticos, indicando para cada evento la entidad que lo causa, la fecha y hora del mismo. La CA debe registrar los eventos relacionados con:

- iniciación y terminación del sistema de certificación;

- los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios de los sistemas de la CA;
- los cambios en la configuración de los sistemas de la CA o en sus claves;
- los cambios en las políticas de creación de certificados;
- los intentos de acceso (login) y de salida del sistema (logoff);
- los intentos no autorizados de acceso a los archivos del sistema;
- la generación de claves de la CA Raíz;
- la emisión y revocación de certificados;
- la generación del CRL;
- los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;
- las operaciones fallidas de escritura o lectura en el repositorio de los certificados y del CRL; y
- las operaciones de escritura en ese repositorio.

La CA debe también registrar, electrónicamente o manualmente informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

- registros de accesos físicos;
- el mantenimiento y los cambios en la configuración de sus sistemas;
- los cambios de personal y los cambios de su rol de confianza;
- los informes de discrepancia y de compromiso;
- el registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados o de la información personal de los usuarios.

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

La CPS debe prever que todos los registros de auditoría, electrónicos o manuales, deberán contener la fecha y hora del evento registrado y la identidad del agente que lo causó.

Para facilitar los procesos de auditoría, toda documentación relacionada a los servicios de la CA, deberá ser almacenada electrónica o manualmente, en un local único, conforme a la política de seguridad de la CA Raíz.

5.4.2 Frecuencia de procesamiento del registro

La CA Raíz debe realizar al menos una revisión de los registros cada 3 (tres) meses.

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

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

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

5.4.3 Período de conservación del registro de auditoría

Las CA deben archivar los registros de auditoría de acuerdo a la sección 5.5.2.

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

5.4.4 Protección del registro de auditoría

Los ficheros de registro, tanto manuales como electrónicos, deben ser protegidos de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada, aplicando controles de acceso lógico y físico. La destrucción de un registro de auditoría solo se puede llevar a cabo con el consentimiento por escrito del personal autorizado.

5.4.5 Procedimientos de respaldo de registro de auditoría

La CA Raíz debe mantener copias de respaldo de todos los registros auditados con una frecuencia, que no debe ser superior a 3 (tres) meses.

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

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

5.4.7 Notificación al sujeto que causa el evento

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

5.4.8 Evaluación de Vulnerabilidades

La CA debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso. Además, se debe evaluar el riesgo a que se expone la organización ante esas vulnerabilidades y se deben tomar medidas para reducir el impacto. Este análisis de riesgo debe ser realizado por la CA Raíz, como mínimo 1(una) vez al año.

5.5 Archivos de registros

5.5.1 Tipos de registros archivados

La CA debe almacenar los registros para establecer la validez de una firma y de la operación propia de la infraestructura PKI. Se deben archivar los siguientes datos:

Durante el inicio de operaciones de la CA:

- documentos requeridos en el inicio de funcionamiento de la CA Raíz.
- la ceremonia de generación de claves de la CA;
- Sus CP y la CPS;
- Cualquier acuerdo contractual para establecer los límites de la CA; y
- La configuración del sistema que requiere la CA.

Durante la operativa de la CA:

- modificaciones o actualizaciones de cualquiera de los ítems anteriores;
- solicitudes de certificados o de revocación;
- documentos requeridos en el procedimiento de habilitación de un PSC;
- documentación para autenticar la identidad del suscriptor;
- documentación de recepción y aceptación del certificado;
- documentación de recepción de dispositivos de almacenamiento de claves;
- todos los certificados y CRL tanto emitidos como publicados;
- registros de auditoría;
- otros datos o aplicaciones para verificar el contenido de los archivos; y
- todos los trabajos comunicados o relacionados a políticas, PSC y cumplimiento de auditoría.

5.5.2 Periodos de retención para archivos

El CRL y los certificados emitidos por la CA Raíz deben ser conservados permanentemente para fines de consulta histórica.

Las copias de los documentos para identificación, presentadas en el momento de la solicitud y de la revocación de certificados, y los acuerdos de suscriptores deben ser conservados, como mínimo, por 10 (diez) años, a contar de la fecha de expiración o revocación del certificado.

Las demás informaciones, inclusive los archivos de auditoría, deberán ser almacenadas, como mínimo, por 10 (diez) años.

5.5.3 Protección de archivos

Los archivos no se deben modificar o eliminar por alguna operación no autorizada de la CA. La misma, debe mantener la lista de personas autorizadas a mover los registros a otros medios.

Los medios de almacenamientos deben estar guardados en instalaciones seguras, los registros deben ser etiquetados con un nombre distintivo, la fecha y hora de almacenamiento y la clasificación del tipo de información.

5.5.4 Procedimientos de respaldo de archivo

La CA debe mantener procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguren la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación de la CA.

La CA debe realizar una segunda copia de todo el material archivado que debe ser almacenada en un local externo a la CA, recibiendo el mismo tipo de protección utilizada para el archivo principal.

Las copias de seguridad deberán seguir los periodos de retención definidos para los registros de las cuales son copias.

La CA Raíz debe verificar la integridad de esas copias de seguridad, como mínimo, cada 6 (seis) meses.

5.5.5 Requerimientos para sellado de tiempo de registros

Los certificados, las listas de revocación (CRL) y otras entradas en las bases de datos de revocación deben contener información de fecha y hora.

5.5.6 Sistema de recolección de archivo (interno o externo)

Los archivos de la CA son de manejo interno de cada una, y se requiere que por lo menos se mantengan dos copias de seguridad, una de las cuales debe ser almacenada fuera del sitio principal de operaciones.

5.5.7 Procedimientos para obtener y verificar la información archivada

Solamente el personal de confianza autorizado está habilitado para obtener acceso al archivo. La CA Raíz debe realizar pruebas de restauración de la información archivada al menos una vez al año. La integridad de la información debe ser verificada cuando es restaurada.

5.6 Cambio de clave

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

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

Nivel de Jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de Suscriptores (Módulo Hardware)	2	2	El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez
Certificado de Suscriptores (Módulo Software)	1	1	El certificado emitido al usuario final es otorgado por un tiempo máximo de un año, al finalizar ese período pierde su validez
Certificado de PSC	8	10	El Certificado emitido al PSC tendrá: Un tiempo operacional de 10 años, que resulta de la suma del tiempo de uso de su certificado (8 años) más el tiempo de validez máximo del certificado de su suscriptor (2 años). Solamente durante el tiempo de uso de su certificado, el PSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional solo podrá firmar el CRL de usuarios o suscriptores.

Certificado CA Raíz	10	20	El Certificado emitido a la CA Raíz tendrá: Un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado (10 años) más el tiempo de validez máximo del certificado de su suscriptor (10 años). Solamente durante el tiempo de uso de su certificado, la CA Raíz podrá emitir certificados a un PSC. En los años restantes del tiempo operacional solo podrá firmar el CRL de PSC.

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

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

Los responsables de las CA tendrán la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7 Recuperación de desastres y compromiso

5.7.1 Procedimiento para el manejo de incidente y compromiso

La CA debe contar con políticas y procedimientos formales para el reporte y atención de incidentes.

Las personas designadas que ejecutan roles de confianza deben velar por la seguridad de las instalaciones y la CA debe mantener procedimientos para que los mismos reporten los incidentes.

La CA debe establecer un plan de contingencia, que permita el restablecimiento y la continuidad del negocio, y la recuperación frente a desastres. Este plan debe contemplar las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación. Dicho plan, debe asegurar que los aspectos básicos del negocio, tales como: servicios de validación o revocación, puedan ser reasumidos en el menor tiempo posible.

Si la CA no puede ser reestablecida dentro de una semana, entonces su clave se reportará como comprometida y todos sus certificados son revocados. En casos excepcionales, la DGFDyCE, puede otorgar extensiones para la CA.

5.7.2 Corrupción de datos, software y/o recursos computacionales

Posterior a una corrupción de recursos computacionales, software o datos, la CA debe realizar, en forma oportuna, un reporte del incidente y una respuesta al evento. Cuando se presentare incidente y compromiso, la CA debe llevar a cabo los procedimientos establecidos en la política de seguridad, plan de contingencia y plan de auditoría o los documentos que los sustituyan para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.3 Procedimientos de compromiso de clave privada de la entidad

El plan de continuidad del negocio de la CA debe considerar el compromiso o sospecha de su clave privada como desastre. En este caso, se prevé la revocación del certificado, la publicación y difusión inmediata.

En el caso de compromiso de la clave privada de la CA Raíz se deberán revocar todos los certificados que se hayan emitido (se procederá a la revocación inmediata de su certificado). Seguidamente, se generará y publicará el correspondiente CRL y notificará a los PSC la revocación del certificado raíz. Para la continuidad de las operaciones se deberá generar un nuevo par de claves y un nuevo certificado raíz autofirmado.

5.7.4 Capacidad de continuidad del negocio después de un desastre

La CA debe desarrollar, probar, mantener e implementar un plan de recuperación de desastres destinado a mitigar los efectos de cualquier desastre natural o producido por el hombre. Los planes de recuperación de desastres se enfocan en la restauración de los servicios de sistemas de información y de las funciones esenciales del negocio.

La CA debe contar y mantener un plan de continuidad de negocios de manera que en el evento de una interrupción del negocio, las funciones críticas puedan ser recuperadas. Para ello la CA debe contar con una instalación de recuperación de desastres en un sitio alterno localizado en una instalación separada geográficamente del sitio principal. Este sitio alterno debe ser diseñado bajo las mismas especificaciones de seguridad que el sitio principal.

En el caso de un desastre que requiera el cese permanente de operaciones del sitio principal de la CA, el equipo técnico conformado y designado para tal caso evaluará la situación y tomará la decisión de declarar formalmente una situación de desastre

y gestionar el incidente. Una vez que es declarada una situación de desastre será iniciada la restauración de la funcionalidad de los servicios de Producción en el sitio alterno.

La CA debe desarrollar un Plan de Recuperación de Desastres para sus servicios administrados. El plan identifica condiciones para la activación del mismo y lo que constituye un tiempo aceptable para la interrupción y recuperación del sistema. El Plan de recuperación de desastres define los procedimientos para que los equipos reconstituyan las operaciones usando datos de respaldo y las copias de respaldo de las claves. Adicionalmente el plan incluye:

- la frecuencia para la toma de copias de seguridad de la información y el software esencial del negocio;
- requisitos para almacenar los materiales criptográficos críticos (por ejemplo, materiales de dispositivo criptográfico seguro y de activación) en una ubicación alternativa;
- La distancia de separación entre el sitio alterno y el sitio principal de la CA; y
- Procedimientos para asegurar la instalación de recuperación de Desastres durante el período de tiempo posterior a un desastre y previo a la restauración de un entorno seguro, ya sea en el sitio original, o uno nuevo.

El plan de recuperación de desastres identifica requisitos administrativos que incluyen:

- programa de mantenimiento para el plan;
- requisitos de sensibilización y educación;
- las responsabilidades de los individuos, y
- la prueba periódica de planes de contingencia.

El sitio alterno, deben tener la capacidad de restaurar o recobrar operaciones esenciales dentro de las veinticuatro horas posteriores al desastre, mínimamente

con soporte para las siguientes funciones: revocación de certificados y publicación de información de revocación.

La CA debe llevar a cabo cuanto menos una prueba de recuperación de desastres por año calendario para asegurar los servicios, en el plan de recuperación de desastres. También debe llevar a cabo anualmente ejercicios de continuidad de negocio formales donde son probados y evaluados procedimientos para tipos adicionales de escenarios (por ejemplo pandemias, inundaciones, apagones entre otros).

Las claves privadas de CA son respaldadas y mantenidas para fines de recuperación de desastre.

5.8 Cese de actividades de una CA

En la eventualidad de que la CA Raíz del Paraguay finalice sus servicios deberá:

- Publicar en su sitio principal de Internet la fecha de finalización de los servicios con al menos 90 (noventa) días de anticipación;
- Publicar la fecha de finalización de sus servicios por el plazo de 3 (tres) días consecutivos en un diario de gran circulación, 10 (diez) días hábiles antes de la suspensión efectiva o cese de las operaciones;
- Notificar al PSC por lo menos 60 (noventa) días antes de la suspensión efectiva o cese de sus operaciones;
- Proceder a la revocación de todos los certificados emitidos que se encuentren vigentes a la fecha de la terminación; y
- Proceder a la destrucción de la clave privada de la CA Raíz del Paraguay mediante un mecanismo que impida su reconstrucción.

Por tanto, finalizado el servicio de la CA Raíz, el PSC no podrá continuar utilizando

el certificado emitido por ella y los terceros aceptantes no deberán confiar en él.

6 CONTROLES TÉCNICOS DE SEGURIDAD

Todos los controles serán aprobados por la DGFDyCE, antes de que se pongan en práctica. En esta sección se definen las medidas de seguridad tomadas por la CA para proteger sus claves criptográficas y los datos de activación. La gestión de las claves es un factor crítico que permite asegurar que todas las claves privadas estén protegidas y solamente pueden ser activadas por personal autorizado.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Conforme a lo estipulado en la CP.

6.1.2 Entrega de la clave privada al suscriptor

Conforme a lo estipulado en la CP.

6.1.3 Entrega de la Clave Pública al emisor del Certificado

Conforme a lo estipulado en la CP.

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

Conforme a lo estipulado en la CP.

6.1.5 Tamaño de la clave

Conforme a lo estipulado en la CP.

6.1.6 Generación de parámetros de clave pública y verificación de calidad

Conforme a lo estipulado en la CP.

6.1.7 Propósitos de usos de clave (Campo Key Usage x509 v3)

Conforme a lo estipulado en la CP.

6.2.1 Estándares y controles del Módulo criptográfico

Conforme a lo estipulado en la CP. Obs.: No se consideran los estándares 14167

Parte 1 y 2.

6.2.2 Control multi-persona de clave privada

Conforme a lo estipulado en la CP.

6.2.3 Custodia de la clave privada

Conforme a lo estipulado en la CP.

6.2.4 Respaldo de la clave privada

Conforme a lo estipulado en la CP.

6.2.5 Archivado de la clave privada

Conforme lo estipulado en la CP.

6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico

Conforme a lo estipulado en la CP.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Conforme a lo estipulado en la CP.

6.2.8 Método de activación de clave privada

Conforme a lo estipulado en la CP.

6.2.9 Métodos de desactivación de la clave privada

Conforme a lo estipulado en la CP.

6.2.10 Destrucción de clave privada

Conforme a lo estipulado en la CP.

6.2.11 Clasificación del Módulo criptográfico

Conforme a lo estipulado en la CP.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

Conforme a lo estipulado en la CP.

6.3.2 Período operacional del certificado y período de uso del par de claves

Conforme a lo estipulado en la CP.

6.4 Datos de activación

Conforme a lo estipulado en la CP.

6.4.1 Generación e instalación de los datos de activación

Conforme a lo estipulado en la CP.

6.4.2 Protección de los datos de activación

Conforme a lo estipulado en la CP.

6.4.3 Otros aspectos de los datos de activación

Conforme a lo estipulado en la CP.

6.5 Controles de seguridad del computador

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Conforme a lo estipulado en la CP.

6.5.2 Clasificación de la seguridad del computador

Conforme a lo estipulado en la CP.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles para el desarrollo del sistema

Conforme lo estipulado en la CP.

6.6.2 Controles de gestión de seguridad

Conforme lo estipulado en la CP.

6.6.3 Controles de seguridad del ciclo de vida

Conforme lo estipulado en la CP.

6.7 Controles de seguridad de red

Conforme lo estipulado en la CP.

6.8. Controles de ingeniería del módulo criptográfico

Conforme lo estipulado en la CP.

7 PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1 Perfil del Certificado

Conforme lo estipulado en la CP.

7.1.1 Número (s) de versión

Conforme lo estipulado en la CP.

7.1.2 Extensiones del certificado

Conforme lo estipulado en la CP.

7.1.3 Identificadores de objeto de algoritmos

Conforme lo estipulado en la CP

7.1.4 Formas del nombre

Conforme lo estipulado en la CP

7.1.5 Restricciones del nombre

Conforme lo estipulado en la CP

7.1.6 Identificador de objeto de Política de Certificado

Conforme lo estipulado en la CP

7.1.7 Uso de la extensión Restricciones de Política (Policy Constraints)

Sin estipulaciones.

7.1.8 Semántica y sintaxis de los Calificadores de Política (Policy Qualifiers)

Conforme lo estipulado en la CP

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

Sin estipulaciones.

7.1.10 Perfiles

Conforme lo estipulado en la CP

7.2 Perfil del CRL

Conforme a lo estipulado en la CP

7.2.1 Número (s) de versión

Conforme a lo estipulado en la CP

7.2.2 CRL y extensiones de entradas de CRL

Conforme a lo estipulado en la CP

7.3 Perfil de OCSP

Conforme a lo estipulado en la CP

7.3.1 Número (s) de versión

Conforme a lo estipulado en la CP

7.3.2 Extensiones de OCSP

Sin estipulaciones.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

De acuerdo al Art. 42 de la Ley Nº 4017/2010 se establece que los PSC, deben ser auditados periódicamente, de acuerdo con el sistema de auditoría que diseñe y apruebe el MIC.

Por Resolución Ministerial se establece el sistema de auditoría al cual será sometido el PSC. Todo PSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la PKI Paraguay. El proceso de auditoría incluye entre otras: Revisión de seguridad y de prácticas, las cuales incluyen instalaciones, documentos de seguridad, declaración de prácticas de certificación, acuerdos entre las partes, política de privacidad y validación de los planes para asegurar el cumplimiento de estándares.

La DGFDyCE o terceros designados por ella, es responsable de ejecutar las auditorías, de acuerdo a lo estipulado en la normativa vigente.

Cada CA, debe implementar un programa de auditorías internas para la verificación de su sistema de gestión.

La disposición o resolución que ordena una auditoría o evaluación no será recurrible.

8.1 Frecuencia o circunstancias de evaluación

La auditoría externa al PSC se debe ejecutar al menos 1 (una) vez al año y los costos deben ser asumidos por el mismo.

De conformidad al programa de auditoría interna, la CA, establecerá la frecuencia o circunstancias para su realización, pero en términos generales se espera que las mismas ejecuten al menos 1 (una) auditoría al año.

8.2 Identificación/Cualificación del evaluador

El equipo de auditoría (interna o externa) debe estar conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de PKI y criptografía.

8.3 Relación del evaluador con la entidad evaluada

Para el caso de las auditorías externas, los auditores deben ser independientes e imparciales y deben ejecutar las evaluaciones acorde a los procedimientos establecidos.

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

8.4 Aspectos cubiertos por la evaluación

Los elementos objeto de Auditoría son:

- Controles de seguridad física y estándares técnicos de seguridad;
- Confidencialidad y calidad de los sistemas de control;
- Integridad y disponibilidad de los datos;
- Cumplimiento de los estándares tecnológicos;
- Seguridad del personal;
- Cumplimiento de la política y declaración de prácticas de certificación;
- Procesos de certificación de clave pública;
- Política de seguridad y privacidad;
- Controles administrativos de la CA;
- Administración de los servicios de la CA;
- Contratos;

- Selección de personal;
- Sistemas de información; y
- Cumplimiento de la legislación vigente, entre otros.

Los detalles de cómo se lleva a cabo la auditoría de cada uno de los elementos están especificados en la **"Guía de estándares tecnológicos y lineamientos de seguridad para la habilitación y auditoría a Prestadores de Servicios de Certificación",** aprobada por resolución ministerial.

8.5 Acciones tomadas como resultado de una deficiencia

La CA debe tener procedimientos para ejecutar acciones correctivas para las deficiencias detectadas tanto en las Auditorías externas como en las internas.

En caso de detectarse una irregularidad en la Auditoría externa realizada al PSC, podrán tomarse entre otras, las siguientes acciones dependiendo de la gravedad de la misma:

- Indicar las irregularidades, pero permitir al PSC que continúe sus operaciones hasta la próxima Auditoría programada.
- Permitir al PSC que continúe sus operaciones con un máximo de 30 (treinta) días corridos, tiempo durante el cual deberá subsanar la irregularidad detectada, caso contrario se procederá a la Suspensión.
- Suspender la operación del PSC.

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

8.6 Comunicación de resultados

La CA debe publicar en el sitio principal de Internet los informes relevantes de las

auditorías realizadas.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

9.1.1 Tarifas de emisión y administración de certificados

Conforme a lo estipulado en la CP.

9.1.2 Tarifas de acceso a certificados

Conforme a lo estipulado en la CP.

9.1.3 Tarifas de acceso a información del estado o revocación

Conforme a lo estipulado en la CP.

9.1.4 Tarifas por otros servicios

Conforme a lo estipulado en la CP.

9.1.5 Políticas de reembolso

Conforme a lo estipulado en la CP.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

La CA, debe contar con un medio de garantía suficiente para cubrir las actividades inherentes a su gestión de conformidad con lo establecido en la normativa vigente.

9.2.2 Otros activos

La CA debe poseer suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes, asimismo debe ser razonablemente capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3 Cobertura de seguro o garantía para usuarios finales

Sin estipulaciones.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

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

- Documentaciones que guardan relación con la solicitud de habilitación como PSC;
- Planes de contingencia y recuperación de desastres;
- Información o documentos que la CA haya determinado como confidencial; y
- Registros de auditoría.

Se debe asegurar la reserva de toda información que mantiene la CA, que pudiera perjudicar la normal realización de las operaciones.

9.3.2 Información no contenida en el alcance de información confidencial

No será considerada información confidencial, el CRL ni la información del estado de los certificados e información que fuera declarada pública por la legislación vigente.

La siguiente información se hará pública por parte de la CA Raíz:

- Los datos de contacto y la razón social de los PSC;
- La información relevante sobre el resultado de la auditoría de los PSC;
- Los requerimientos para la acreditación de los PSC;
- Las resoluciones mediante las que se habilita, revoca o deniega a un PSC;
- La compañía con la que contrató la póliza de seguro;
- El certificado del PSC;
- El certificado de la CA Raíz;
- La información referida a la revocación de un certificado publicada por la CA Raíz a través de su CRL, disponible en el sitio

https://www.acraiz.gov.py/arl/ac_raiz_py.crl.

9.4 Privacidad de información personal

9.4.1 Plan de Privacidad

La CA está obligada a garantizar la protección, la confidencialidad y el debido uso de la información suministrada por los suscriptores de los servicios de certificación.

9.4.2 Información tratada como privada

Cualquier información acerca de los suscriptores que no esté públicamente disponible a través del contenido del certificado emitido y servicios de CRL y OCSP, debe ser tratada como información privada. La información relativa al suscriptor que describa su infraestructura tecnológica o de procesos internos de negocio deberá tratarse como privada.

9.4.3 Información que no es considerada como privada

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

9.4.4 Responsabilidad para proteger información privada

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

El personal que desempeñe labores en la CA y toda persona que tenga acceso a los datos considerados privados se encuentra constreñida a proteger la información y debe estar obligado contractualmente a ello.

9.4.5 Notificación y consentimiento para usar información privada

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

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del suscriptor o de cualquier otra información generada o recibida durante el ciclo de vida del certificado, solo se hará efectiva previa autorización de dicho suscriptor. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público.

9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo

La condición de información secreta, por ley, reservada o confidencial cesa ante la solicitud de juez competente en el marco de un proceso jurisdiccional que así lo determine y se divulgará estrictamente la información solicitada.

9.4.7 Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales la CA divulgue información.

9.5 Derecho de Propiedad intelectual

La CA, debe mantener en forma exclusiva todos los derechos de propiedad intelectual, con respecto a la presente documentación y aplicaciones pertenecientes a ella.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

La CA Raíz debe garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión de los mismos;

- No existan errores en la información que fue introducida por la entidad que aprueba la emisión del certificado;
- Los certificados reúnen los requerimientos expuestos en la CP y CPS;
- Los servicios de revocación y el uso de los repositorios cumplen lo estipulado en la CP y CPS;
- Asegurar la protección de su clave privada ;
- Verificar que el PSC cumple los requisitos para ser integrante de la PKI Paraguay;
- Publicar en el sitio principal de Internet la CP y CPS de la CA Raíz; asimismo los datos del PSC requeridos en la norma;
- Asegurar que su clave pública, la CPS, CP y otros documentos de carácter público, estén disponibles para cualquier interesado que lo requiera;
- Garantizar la adopción de las medidas necesarias para evitar la falsificación de los Certificados digitales que proporcionen;
- Realizar auditorías internas;
- Revocar el certificado de un PSC cuando existan motivos para ello;
- Mantener un registro actualizado de los certificados de los PSC que han sido otorgados o revocados; y
- Garantizar y proteger sus claves privadas en dispositivos criptográficos que cumplan con la FIPS 140-2 Nivel 3.

9.6.2 Representaciones y garantías de la RA

Las CA en su función de Registro debe asegurar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No se presentan errores en la información del certificado que fue introducida por las entidades de registro.

- Que los dispositivos y materiales requeridos cumplen con lo dispuesto en la CP y CPS.
- Realizar sus operaciones de conformidad con la CPS y la CP;
- Comprobar exhaustivamente la identidad del suscriptor para lo que se requerirá la presencia física del mismo.
- No almacenar ni copiar datos de creación de firma del titular del certificado;
- Informar al PSC antes de su habilitación, sobre las obligaciones que asume, entre las cuales se encuentran las siguientes:

  - ✓ La forma en que debe custodiar los datos de creación de firma;
  - ✓ El procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma;
  - ✓ De las tasas y aranceles;
  - ✓ De las condiciones precisas para la utilización del certificado;
  - ✓ De sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial;
  - ✓ Conocer el sitio web donde puede consultar cualquier información de la CA Raíz, la CPS y la CP vigentes y anteriores;
  - ✓ Conocer la legislación aplicable.

- Formalizar el acuerdo de suscriptores;
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada;
- En el caso de la aprobación de una solicitud de habilitación notificar al solicitante;
- En el caso del rechazo de una solicitud de habilitación, notificar al solicitante dicho rechazo y su motivo;
- Mantener bajo su estricto control las herramientas de tramitación de certificados electrónicos;
- Recibir y tramitar las solicitudes de habilitación o emisión de certificado que reciba;

- Recibir y tramitar las solicitudes de revocación que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable del solicitante, basadas en la normativa.

9.6.3 Representaciones y garantías del suscriptor

El PSC como suscriptor de la CA Raíz debe garantizar que:

- La clave privada está protegida y que no autoriza a otras personas tener acceso a la misma;
- Toda la información facilitada por el suscriptor y contenida en el certificado, es verdadera;
- El certificado es utilizado exclusivamente para los propósitos autorizados;
- Tener conocimiento de los pasos necesarios para la habilitación ante el MIC;
- Actuar con diligencia para evitar el uso no autorizado de su clave privada;
- Garantizar y proteger sus claves privadas en dispositivos criptográficos que cumplan con la FIPS 140-2 Nivel 3;
- Notificar a la CA Raíz que su clave privada ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello; y
- Elaborar su propia CPS y CP, que deberán ser acordes a las directivas dictadas por la CA Raíz.

9.6.4 Representaciones y garantías de las partes que confían

Las partes que confían requieren conocer suficiente información para tomar la decisión de aceptar el certificado.

9.6.5 Representaciones y garantías de otros participantes

Sin estipulaciones.

9.7 Exención de garantía

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

La CA no asume ninguna responsabilidad en caso de cualquier tipo de pérdida o perjuicio:

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

9.8 Limitaciones de responsabilidad legal

A excepción de lo establecido por las disposiciones de la presente CPS, en la normativa vigente y sus reglamentos, la CA Raíz no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían.

9.9 Indemnizaciones

La CA debe indemnizar a los suscriptores por cualquier causa legalmente establecida, se deberá demostrar ante las autoridades correspondientes los daños y perjuicios causados por ella.

9.10 Plazo y finalización

9.10.1 Plazo

La CPS de la CA Raíz empieza a ser efectiva en la fecha estipulada en la Resolución Ministerial de aprobación expedida por el MIC.

9.10.2 Finalización

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

9.10.3 Efectos de la finalización y supervivencia

La finalización de la vigencia de la CPS, puede ser por derogación expresa, enmiendas o modificaciones; todos los certificados emitidos bajo esa política seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Política contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

9.11 Notificación individual y comunicaciones con participantes

Toda comunicación entre la CA y el suscriptor, se realizará mediante mensaje de datos firmado digitalmente o documento escrito dirigido a cualquiera de las

direcciones establecidas como contacto. Las comunicaciones electrónicas se harán efectivas una vez que la reciba el destinatario al que van dirigidas, de igual manera en el caso de las escritas.

9.12 Enmiendas

9.12.1 Procedimientos para enmiendas

La DGFDyCE está facultada a introducir enmiendas o modificaciones, las que deberán ser documentadas y mantenerse a través de versiones y publicadas en el sitio de Internet de la CA Raíz. Por Resolución Ministerial, se fijará el plazo al cual, el PSC deberá ajustarse a la nueva versión.

9.12.2 Procedimiento de publicación y notificación

Toda enmienda o modificación de la CPS, se publicará en el sitio principal de Internet de la CA.

9.12.3 Circunstancias en que los OID deben ser cambiados

Sin estipulaciones

9.13 Disposiciones para resolución de disputas

En la eventualidad de cualquier disputa que implique los servicios o prestaciones que incluye la CP, CPS y normativa vigente, la parte afectada notificará primero a la CA y a todas las partes interesadas con relación a la disputa. La CA, asignará al personal adecuado para resolver en lo posible el litigio extrajudicialmente.

9.14 Normativa aplicable

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

9.15 Adecuación a la ley aplicable

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

9.16 Disposiciones varias

9.16.1 Acuerdo completo

No aplica

9.16.2 Asignación

No aplica

9.16.3 Divisibilidad

En el eventual caso que una cláusula de la CPS sea declarada inconstitucional por la Corte Suprema de Justicia, el resto de las cláusulas de estas políticas se mantendrán vigentes.

9.16.4 Aplicación (Honorarios de Abogados y renuncia de derechos)

No aplica

9.16.5 Fuerza mayor

Los Acuerdos de Suscriptores deben incluir cláusulas de fuerza mayor para proteger a la CA.

9.17 Otras disposiciones

El PSC habilitado de conformidad a los términos de la CPS derogada, deberá adecuarse a las disposiciones de la presente CPS en el plazo establecido por la Resolución que la ponga en vigencia.

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 Nº 4017/2010 ‘’De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico’’.
- Ley Nº 4610/2012 que modifica y amplía la Ley Nº 4017/2010.Decreto Reglamentario Nº 7369/2011.