DECLARACION DE PRACTICAS CERTIFICACIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA DEL PARAGUAY

Ministerio de Industria y Comercio

Viceministerio de Comercio

República del Paraguay

Tabla de contenido

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 (DGFD&CE) es la dependencia designada para ejecutar las funciones atribuidas al MIC como AA.

Entre sus funciones principales se encuentran:

- Administrar la Autoridad Certificadora Raíz del Paraguay (CA Raíz)
- Dictar las normas que regulen el Servicio de Certificación Digital en el país
- Estudiar la Solicitud de Habilitación del Prestador de Servicios de Certificación (PSC) y emitir dictamen técnico-jurídico de aprobación o rechazo
- Auditar al PSC
- Evaluar la posible revocación de la Habilitación del PSC
- Imponer sanciones al PSC

La Habilitación del PSC, será aprobada por resolución ministerial, previo dictamen de la DGFD&CE, al igual que la revocación de su habilitación.

La presente Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement), describe las prácticas y procedimientos empleados por la DGFD&CE en el desempeño de sus funciones como administradora de la Autoridad Certificadora Raíz (CA Raíz) y establece los términos bajo los cuales será prestado el servicio de certificación digital.

La estructura de 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 el PSC, el uso de los certificados digitales, entre otras cuestiones relacionadas con la PKI Paraguay.

Esta CPS se define de acuerdo con los requisitos establecidos en la Política de Certificación (CP). El Prestador de Servicios de Certificación (PSC), debe contar con una CP y CPS cuyo contenido debe concordar con las disposiciones establecidas en el presente documento y la CP de la PKI.

En resumen, esta CPS es específicamente aplicable a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz)
- Prestador de Servicios de Certificación (PSC)
- Usuario Final
- Parte que confía

Esta CPS contempla los siguientes tipos de certificados:

- Certificado de CA Raíz
- Certificado de PSC
- Certificado de persona física para autenticación
- Certificado de persona física para firma digital
- Certificado de persona jurídica para autenticación
- Certificado de persona jurídica para firma digital

El certificado de CA Raíz cuenta con el nivel más alto en la jerarquía de PKI Paraguay; el mismo contiene la clave pública correspondiente a la clave privada de la CA Raíz que es utilizada para firmar:

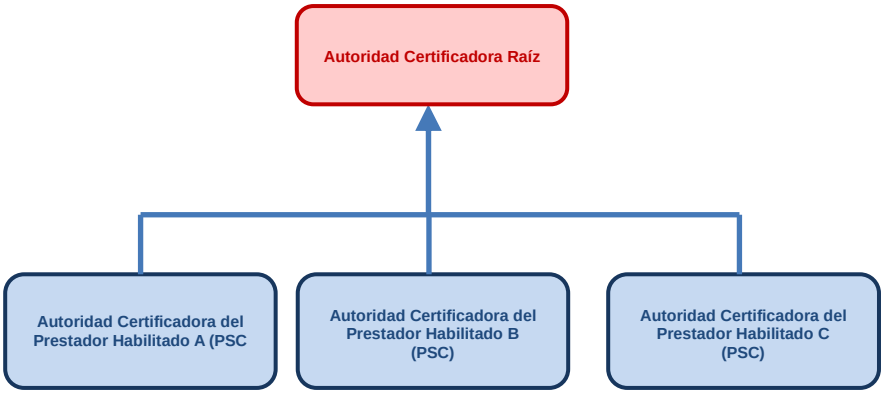
- su propio certificado;
- certificados de CA inmediatamente inferior a su nivel; y

- su Lista de Certificados Revocados (CRL).

El PSC, una vez habilitado, pasará a formar parte de la cadena de confianza de la PKI Paraguay, para lo cual deberá contar con un certificado digital firmado y emitido por la CA Raíz, conformando de esa 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, habilitados a emitir certificados digitales a usuarios finales.

Figura 1



1.2 Nombre e Identificación del documento

Nombre: Declaración de Prácticas de Certificación de la Infraestructura de Clave Pública del Paraguay

Versión: 3.0

Fecha de aprobación:_____febrero de 2014

Sitio de internet oficial: www.acraiz.gov.py/cps/dpc_acrp.pdf

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras (CA)

Son las entidades autorizadas a emitir certificados de clave pública dentro de la PKI Paraguay. Esto incluye a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz)

La CA Raíz es administrada por la AA y sus funciones están estipuladas en la CP, en la presenta CPS y normativa vigente.

- Prestador de Servicios de Certificación (PSC)

La entidad interesada en prestar servicios de certificación digital deberá presentar la Solicitud de Habilitación al MIC y además deberá ajustarse al procedimiento establecido para el efecto.

1.3.2. Autoridad de Registro (RA)

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

- Que el trámite se realice de forma presencial por parte de las personas implicadas en la solicitud, custodia y uso del certificado solicitado, en todas las modalidades del certificado;
- 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;
- 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 y suscribir con el usuario solicitante el Formulario de Solicitud respectivo. Deberá hacer entrega de la copia del Acuerdo de Suscriptores y posteriormente entregar el certificado solicitado.

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. Es obligación de todo suscriptor el conocimiento de la presente CPS así como de la normativa vigente.

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

La CP es la que determina los usos apropiados que deben darse al certificado, no es objetivo de esta CPS la determinación de dicho usos.

Para una mayor claridad, se describen los valores del campo Uso de la Clave - ‘’Key Use’’ utilizado en los diferentes tipos de certificados:

- Firma de Certificado (Certificate Signing): se usa en caso que la clave pública del suscriptor es utilizada para verificar una firma en certificados. Esta extensión solo se puede utilizar en los certificados de CA. Si el Certificate Signing se activa, en la extensión del perfil restricciones básicas deberá aparecer la restricción tipo de sujeto (subject type) = CA;
- Firma CRL (CRL Signing) y Firma del CRL sin conexión (Off line CRL Signing): se activa cuando la clave pública del suscriptor se utiliza para la verificación de firmas en la lista de revocación de certificados;
- Firma Digital (Digital Signature): se activa cuando la clave pública del suscriptor se usa para la verificación de firmas digitales, distintas de firmas en certificados;
- No repudio (Non repudiation): se activa cuando la clave pública del suscriptor es utilizada para verificar las firmas digitales, distintas de las firmas en certificados, proporciona un servicio de no repudio que protege contra el hecho que el firmante falsamente niegue alguna acción. En las últimas ediciones de X.509 han cambiado el nombre del no repudio a contenido aprobado (Content commitment);
- Cifrado de Clave (Key encipherment): se activa cuando la clave pública del suscriptor es utilizada para cifrar otras claves usadas en proceso de autenticación. No se encriptan los datos. Acuerdo de Clave (Key agreement): se activa cuando la clave pública del suscriptor es utilizada para acordar la clave.

1.4.2. Usos prohibidos del certificado

La CP 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 Política de Administración

1.5.1. Organización que administra el documento

Nombre: Dirección General de Firma Digital y Comercio Electrónico (DGFD&CE).

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

Teléfono: (+595) (21) 616-3000.

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

Página Web: www.acraiz.gov.py.

1.5.2. Persona de Contacto

Nombre: Dirección General de Firma Digital y Comercio Electrónico (DGFD&CE).

Dirección: Avenida Mcal. López N° 3333. 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

El Director General de Firma Digital y Comercio Electrónico, será el encargado de determinar la adecuación de la Declaración de Prácticas de Certificación (CPS) de la PKI y la del PSC que desee formar parte de la PKI Paraguay.

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

El MIC aprobará el contenido de la presente Declaración de Prácticas de Certificación y sus posteriores enmiendas o modificaciones, por Resolución Ministerial.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

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

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): Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio. órgano regulador competente designado por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 “De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico”.

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

Autoridad Certificadora Raíz (CA Raíz): Es la Autoridad de Certificación Raíz de la PKI

Paraguay, cuya función principal es habilitar al PSC y emitirle certificados digitales. Posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Identificador de Objeto (OID): 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 documentos 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 que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos bajo la PKI Paraguay.

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

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

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

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

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

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

Prestador de Servicios de Certificación (PSC): Entidad habilitada ante la AA, encargada de

operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz y solo podrá emitir certificados a usuarios finales.

Registro de Auditoría: Registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.

Repositorio: Sitio principal de internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.

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

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

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

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 (del inglés, Country)
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CIE	Cédula de identidad extranjera
CN	Nombre común (del inglés, Common Name)
CP	Políticas de Certificación (CP por sus siglas en inglés Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement)

Acrónimo	Descripción
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)
CSP:	Prestadores de Servicios de Certificación (CSP por sus siglas en inglés Certification Service Provider)
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 Workshopp Agreement)
DGFD&CE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio.
DNS	Servicio de nombre de dominio (DNS por sus siglas en inglés Domaine Name server)
ETSI	Instituto Europeo de Normas de Telecomunicaciones (ETSI por sus siglas en inglés European Telecomunications Standards Institute)
FIPS	Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés Federal Information Processing Standards).
HSM	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 Telecomunication Union – Telecomunication Standardization Sector)

Acrónimo	Descripción
MIC	Ministerio de Industria y Comercio
O	Organización (del inglés Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés Online Certificate Status Protocol).
OID	Identificador de Objeto (OID por sus siglas en inglés Object Identifier).
OU	Unidad Organizacional (OU, por sus siglas en inglés Organization Unit)
PIN	Número de Identificación Personal, (por sus siglas en inglés Personal Identification Number) contraseña que protege el acceso a una tarjeta criptográfica
PKCS	Norma de criptografía de clave pública (PKCS por sus siglas en inglés Public Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés Public Key Infrastructure).
PSC	Prestador de Servicios de Certificación
PY	Paraguay
RA	Autoridad de Registro (RA por sus siglas en inglés Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés Request for Comments)
RSA	Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman
RUC	Registro único del Contribuyente
SN	Número de Serie (del inglés, Serial Number)

Acrónimo	Descripción
SSL	Capa de Conexión Segura (SSL por sus siglas en inglés Secure Sockets Layer)
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).

2 RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

2.1. Repositorios

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

De la misma manera, el PSC debe contar con un sitio de internet como repositorio público de información, el cual deberá ser verificado al momento de la Habilitación.

2.2 Publicación de Información de Certificación

Además de lo establecido en la CP sobre el contenido de la publicación de la información, la CA debe garantizar que todos los certificados de la cadena de confianza estén publicados y disponibles en el sitio principal de internet.

El servicio de publicación de información de una CA debe 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. La CA dedicará sus mejores esfuerzos para que el servicios se restablezca y esté disponible rápidamente.

2.3 Tiempo o frecuencia de Publicación

Conforme lo estipulado en la CP.

2.4 Controles de Acceso a los Repositorios

La CA debe implementar medidas de seguridad lógicas y físicas para evitar que personas no autorizadas puedan añadir, borrar o modificar el contenido del repositorio.

3 IDENTIFICACION Y AUTENTICACION

3.1 Nombres

3.1.1 Tipos de Nombres

Conforme lo estipulado en la CP.

3.1.2. Necesidad de Nombres significativos

Conforme lo estipulado en la CP.

3.1.3. Anonimato o seudónimos de los suscriptores

Conforme lo estipulado en la CP.

3.1.4 Reglas para interpretación de varias formas de Nombres

Certificado de PSC, Certificado de Persona Jurídica para firma digital y para autenticación

Conforme a lo estipulado en la CP.

Certificado de Persona física para firma digital y para autenticación

Conforme a lo estipulado en la CP.

3.1.5 Unicidad de los nombres

Conforme lo estipulado en la CP.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

Conforme a lo estipulado en la CP.

3.2 Validación inicial de identidad

En las siguientes subsecciones se describen los procedimientos y criterios para validar la identidad y/o otros atributos de un solicitante de certificado. Se debe asegurar la verificación presencial de la identidad del solicitante de un certificado.

3.2.1 Método para probar posesión de la clave privada

Conforme lo estipulado en la CP.

3.2.2 Autenticación de identidad de Persona Jurídica

El proceso de comprobación de la identidad de la persona jurídica cuyos datos se incluyen en un certificado tiene como objeto garantizar que el titular del certificado sea la misma persona jurídica identificada en la solicitud de un certificado, y que la información que se incluye en el certificado sea verdadera y exacta.

La CA como mínimo deberá requerir la presentación de los siguientes documentos respaldatorios:

- Documento que acredite la creación de la persona jurídica.
- RUC
- Nombre y documento de identidad del representante legal
- Domicilio de la persona jurídica

3.2.3 Autenticación de identidad de Persona Física

El proceso de comprobación de la identidad de la persona física cuyos datos se incluyen en un certificado tiene como objeto garantizar que el titular del certificado sea la misma persona identificada en la solicitud de un certificado, y que la información que se incluye en el certificado sea verdadera y exacta. Se debe verificar la identidad del solicitante mediante la exhibición del documento original de identidad expedido por el Departamento de Identificaciones de la Policía Nacional, el cual deberá estar vigente al momento de la presentación.

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 interoperabilidad

Conforme lo estipulado en la CP.

3.3 Identificación y autenticación para solicitudes de re emisión de claves

3.3.1 Identificación y autenticación para re emisión de claves rutinaria

No se permite la re emisión de claves

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

No se permite la re emisión de claves

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 lo estipulado en la CP

4.1.2 Proceso de Inscripción y responsabilidades

Conforme lo estipulado en la CP

4.2. Procesamiento de la Solicitud del Certificado

4.2.1 Ejecución de las funciones de Identificación y Autenticación

La CA en su función de Registro debe especificar como mínimo los siguientes procedimientos para la validación de identidad de una persona física o jurídica:

- El solicitante del certificado debe asistir personalmente para la verificación de su identidad
- Indicar el lugar donde se realizará la verificación
- Designar a la persona responsable de la verificación
- Requerir la documentación necesaria para identificar a una persona según sea una persona física, jurídica o PSC
- Comprobar la veracidad de las documentaciones presentadas a través de consultas a bases de datos oficiales de información nacional y registros públicos.

4.2.2 Aprobación o rechazo de solicitudes de certificado

La solicitud del certificado no trae implícita su obtención, razón por la cual si el solicitante no cumple con los requerimientos establecidos en la normativa, será rechazado; la CA no contrae responsabilidad alguna por las consecuencias derivadas del rechazo.

En el caso que una solicitud sea aprobada por la CA, ésta debe realizar lo siguiente:

- Proceder a la emisión del certificado
- Requerir al suscriptor la firma de un contrato de conformidad personal (acuerdo de suscriptores).

El contrato antes aludido deberá contener responsabilidades y las obligaciones que deben cumplir los suscriptores de conformidad con la legislación que rige la materia, para garantizar el efecto legal de las transacciones realizadas empleando el certificado emitido por dicha CA, así como las consecuencias de no cumplir con el acuerdo.

El contrato del suscriptor puede ser firmado de forma digital o manuscrita y debe ser archivado por la CA. La CA debe registrar y archivar toda información proporcionada por los solicitantes, lo cual incluye el acuerdo de suscriptor

4.2.3. Tiempo para procesar solicitudes de Certificado

Para el PSC

El tiempo de procesamiento del CSR, será como máximo de cinco días hábiles contados a partir de la Resolución Ministerial de Habilitación.

Para persona física y jurídica

Se establece el plazo máximo de cinco días hábiles para la tramitación de la solicitud del certificado, contados a partir de haberse verificado la identidad del solicitante y admitida la solicitud. En caso que la CA supere el plazo máximo establecido para la tramitación de la solicitud, deberá informar al solicitante de las causas que motivaron la demora y el nuevo

plazo en el que se tramitará la solicitud. En caso que el interesado opte por desistir de su solicitud por el motivo expuesto, la CA tendrá previsto un procedimiento de reembolso de lo abonado.

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 lo estipulado en la CP.

4.4. Aceptación del Certificado

4.4.1 Conducta constitutiva de aceptación de certificado

Conforme lo estipulado en la CP

4.4.2 Publicación del Certificado por la CA

La CA Raíz debe publicar en su sitio principal de Internet su certificado. El PSC, debe publicar su certificado y el certificado de la CA Raíz para validar la cadena de confianza de la PKI Paraguay.

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

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

4.5 Uso del par de claves y del certificado

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

Las responsabilidades y limitaciones del uso del par de claves y del certificado se establecen en la correspondiente CP.

De forma general cabe mencionar que el suscriptor solo puede utilizar la clave privada y el certificado para los usos autorizados en la CP y de acuerdo con lo establecido en los Campos ‘’Uso de la Clave (Key usage) ’’ y ‘’Uso extendido de la Clave (Extended key usage)’’del Certificado.

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

Los terceros que confían solo pueden depositar su confianza para aquello que establezca la correspondiente CP y de acuerdo con lo establecido en los campos ‘’Uso de la Clave (Key usage) ’’ y ‘’Uso extendido de la Clave (Extended key usage)’’del Certificado.

Los terceros aceptantes han de realizar las operaciones de la clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta CPS y en la CP.

4.6 Renovación del certificado

Conforme lo estipulado en la CP.

4.6.1 Circunstancias para renovación de certificado

No aplica.

4.6.2 Quién puede solicitar renovación

No aplica.

4.6.3 Procesamiento de solicitudes de renovación de certificado

No aplica.

4.6.4 Notificación al suscriptor sobre la emisión de un nuevo certificado

No aplica.

4.6.5 Conducta constitutiva de aceptación de un certificado renovado

No aplica.

4.6.6 Publicación por la CA del certificado renovado

No aplica.

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

No aplica.

4.7 Re-emisión de claves de certificado

Conforme 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

Conforme lo estipulado en la CP.

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

Se procederá a la revocación por:

a) Circunstancias que afecten la información contenida en el certificado:

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento que algunos de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
- Descubrimiento que algunos de los datos contenidos en el certificado es incorrecto

b) Circunstancias que afectan la seguridad de la clave o del certificado

- Compromiso de la clave privada o de la infraestructura o sistemas de la CA que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
- Infracción, por la CA, de los requisitos previstos en los procedimientos de gestión de los certificados, establecidos en la PC y CPS de la CA.

- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor
- Acceso o utilización no autorizada, por un tercero, de la clave privada del suscriptor
- El uso irregular por el suscriptor, o falta de diligencia en la custodia de la clave privada

c) Circunstancias que afectan la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico
- Pérdida o inutilización por daños del dispositivo criptográfico
- Acceso no autorizado, por un tercero, a los datos de activación del suscriptor

d) Circunstancias que afectan al suscriptor

- Extinción del acuerdo de suscriptores
- Infracción por el suscriptor de los requisitos pre establecidos para la solicitud del certificado
- Infracción por el suscriptor de sus obligaciones, responsabilidad y garantías, establecidas en la CP y CPS de la CA que emitió el certificado.
- La incapacidad sobrevenida o la muerte del suscriptor
- La extinción de la persona jurídica suscriptora del certificado
- Solicitud del suscriptor de revocación del certificado de acuerdo con lo establecido en la CP y en la CPS.
- Otras causales especificadas en la normativa y reglamentación vigente.

De presentarse y constatarse las circunstancias de revocación mencionadas en el punto 4.9.1 de la CP y las indicadas más arriba, la CA procederá de oficio a la revocación de los certificados de sus suscriptores.

4.9.2 Quien puede solicitar Revocación

Conforme lo estipulado en la CP.

4.9.3 Procedimiento para la solicitud de revocación

Sin perjuicio de lo establecido en la CP, la solicitud de revocación podrá ser:

- Presencial: a través de los procesos de autenticación, de identidad indicados en la CP.
- Correo electrónico: la solicitud de revocación tendrá que ser firmada digitalmente por el solicitante, siempre que lo haga con un certificado vigente, salvo que la clave privada se encuentre en entredicho, en cuyo caso la solicitud de revocación solamente podrá hacerse en forma presencial

La solicitud de revocación deberá contener como mínimo la siguiente información:

- Fecha de solicitud de la revocación
- Identidad del suscriptor
- Causa de la solicitud de la revocación
- Identidad de la persona que solicita la revocación
- Datos de contacto de la persona que solicita la revocación

La solicitud de revocación presentada será evaluada para su admisión o rechazo por la DGFD&CE, quien procederá conforme a un Dictamen Técnico.

En caso que el PSC a quien se le ha revocado su certificado, desee no obstante seguir operando como tal, y si no existe impedimento o prohibición, deberá solicitar nuevamente ante el MIC presentando las documentaciones indicadas en la normativa y reglamentación vigente para la habilitación.

Se comunicará al suscriptor, la revocación de su certificado a la dirección de correo

electrónico declarada como medio de contacto para las notificaciones correspondientes. La solicitud de revocación de un certificado recibida con posterioridad a su fecha de expiración no será tramitada.

Un certificado revocado no puede volver a utilizarse, vale decir que no puede levantarse la revocación, ni anularse de ninguna otra forma. Cuando un certificado es revocado todas sus instancias son revocadas, constituye un estado definitivo del certificado.

4.9.4 Periodo de gracia para solicitud de revocación

No se estipula periodo de gracia.

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

Conforme lo estipulado en la CP.

4.9.6 Requerimientos de verificación de revocación para las partes que confían

Conforme lo estipulado en la CP.

4.9.7 Frecuencia de Emisión del CRL

Conforme lo estipulado en la CP.

4.9.8 Latencia máxima para CRLs

Conforme lo estipulado en la CP.

4.9.9 Disponibilidad de verificación de revocación/ estado en línea

Los terceros que confían deberán comprobar el estado de aquellos certificados en los que desean confiar.

Una forma por la que se puede verificar el estado de los certificados es consultando la CRL o Delta-CRL más reciente emitida por la CA que expidió el certificado en el que se desea

confiar, que deberá estar disponible en su sitio principal de internet. Adicionalmente el PSC debe implementar el servicio de validación en línea OCSP.

En el caso que no fuera posible verificar el estado de un certificado, los terceros que confían en él deberán desestimar su uso por el grado de responsabilidad, el riesgo que representa y por las consecuencias que pudiere producir.

4.9.10 Requerimientos para verificar la revocación en línea

La parte que confía debe verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección anterior.

4.9.11 Otras formas de advertencias de revocación disponibles

Sin estipulaciones

4.9.12 Requerimientos especiales por compromiso de clave privada

El compromiso de la clave privada de una CA será notificado, en la medida posible, a todos los participantes de la PKI Paraguay, en especial a:

- Todos los suscriptores de certificados emitidos por esa CA
- Terceros que confían, los que se tenga conocimiento

Además la CA deberá publicar el compromiso de su clave en su sitio principal de internet y procederá a la inmediata gestión de la revocación de su certificado y el de sus suscriptores. La CA, publicará el certificado revocado en el repositorio.

En caso de haberse revocado el certificado de la CA Raíz y subsanada la circunstancia que la motivó, ésta debe:

- Generar su nuevo certificado
- Emitir un nuevo certificado para el PSC habilitado

- Asegurar que todos los nuevos certificados emitidos por el PSC estén firmados con la nueva clave

En el caso de que la clave privada comprometida sea de la CA Raíz, se eliminará el certificado de todas las aplicaciones y se distribuirá uno nuevo.

En caso de haberse revocado el certificado del PSC y subsanada las circunstancias que la motivó, ésta debe:

- Solicitar nuevamente su habilitación
- Emitir un nuevo certificado a sus suscriptores

El plan de continuidad del negocio del PSC deberá establecer que en el caso de compromiso de su clave, el certificado asociado será inmediatamente revocado, igualmente serán revocados todos los certificados que hayan sido emitidos con ese certificado, ofreciendo a los usuarios finales, la posibilidad de disponer de un nuevo certificado emitido gratuitamente por un periodo igual al de la vigencia del certificado revocado del suscriptor..

4.9.13 Circunstancias para suspensión

Según la normativa no se aplica la suspensión del Certificado.

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 lo estipulado en la CP.

4.10.2 Disponibilidad del Servicio

Conforme lo estipulado en la CP.

4.10.3 Características opcionales

Sin estipulaciones

4.11 Fin de la suscripción

Conforme 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 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

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

Además de lo estipulado en la CP, las instalaciones en las que se procesa información deben

cumplir los siguientes requisitos físicos:

- El edificio que contiene las unidades de procesamiento de información debe ser físicamente sólido, los muros externos deben ser de construcción sólida dotado 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 deberán 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 en la CP.
- Los equipos informáticos (principal y alterno) deben estar instalados en centros de datos que cuenten con medidas de seguridad necesarias conforme lo señalado en la CP.
- Los sistemas deben estar están físicamente separados de otros existentes en el lugar, de forma que solo el personal autorizado de la CA pueda acceder a ellos, garantizando así la independencia de otros equipos y sistemas de terceros alojados en el lugar.
- Las instalaciones deben contar cuanto menos 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 debe situarse en zona de bajo nivel de delincuencia
    - El edificio debe encontrarse en una zona sin antecedentes de catástrofes naturales y de baja actividad sísmica.

- Ni el edificio, ni la zona donde se encuentran, deben estar considerados como objetivo terroristas.
- El sitio donde se encuentran las claves privadas de la CA debe estar protegido constantemente por personal perteneciente a una institución de seguridad autorizada especialmente. Este personal tiene información detallada y actualizada de las personas que la CA autoriza a acceder al núcleo central donde se encuentran los equipos informáticos de la CA. En ningún caso deben permitir la extracción de equipamientos sin autorización expresa.
- El acceso al núcleo central de servidores de confianza se debe realizar superando distintos controles conforme a lo indicado en la CP. El personal que accede se debe encontrar en todo momento acompañado por personal responsable de la administración del centro de datos y cualquier labor que realiza sobre los equipos informáticos de CA debe ejecutarse en presencia constante de un técnico perteneciente al personal responsable de la administración del centro de datos.
- Sistema de energía y aire acondicionado redundantes, que cumplan con las normas industriales, a fin de crear un entorno operativo adecuado.
- Mecanismos de prevención destinados a reducir el efecto del contacto con el agua.
- Mecanismos de prevención y protección contra incendios, que cumplan con las normas industriales.
- Todo el cableado debe estar protegido contra daños o interceptación electromagnética o interceptación de la transmisión tanto de datos como de telefonía.

5.1.2 Acceso físico

- Perímetro de seguridad física

Se debe establecer que el personal visitante esté permanentemente tutelado por un personal de la CA conforme lo estipulado en la CP.

- Controles físicos de entrada

Se debe contar con un exhaustivo sistema de control físico de personas a la entrada y a la salida de conformidad a los perímetros de seguridad establecido en la CP.

Se combinan diversos sistemas de seguridad, humanos y técnicos, en la realización de controles físicos de entrada:

- Acceso a la entrada identificándose mediante CI ante los servicios de seguridad, monitoreando y registrando personas, la hora de llegada, salida, autorización que ostenta y dotado de una tarjeta de identificación o de visitante.
- Uso de tarjeta de identificación ante dispositivos de seguridad, comprobando autorización y registrando acceso.

- Introducción y extracción de equipos

Se requiere autorización expresa de la CA para la realización de estas operaciones, llevando un inventario del material existente y de las entradas y salidas que se han producido.

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. Como mínimo 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 Data Center, incluido los equipos informáticos y equipos de refrigeración.

5.1.4 Exposiciones al agua

Además de lo estipulado en la CP, las instalaciones de la CA deben estar protegidas para evitar exposiciones al agua de las mismas, 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.

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 resistencia:

- Al fuego por al menos 60 minutos
- 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.

5.1.7 Eliminación de residuos

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 es 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.

5.2 Controles procedimentales

5.2.1 Roles de confianza

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

a. Responsable de las prácticas de seguridad de la CA (Coordinador de Seguridad):

Debe llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobadas por la CA, controlar la formalización de los convenios entre el personal y la CA, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, debe cumplir y hacer cumplir las políticas de seguridad de la CA y debe encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Es el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls Debe comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a estos, asimismo debe resolver o hacer que resuelvan las incidencias de seguridad

producidas, de eliminar vulnerabilidades detectadas, etc. y es el encargado de la gestión y control de seguridad física, y de los movimientos de material fuera de las instalaciones de la CA

b. **Responsable de la aprobación de la emisión y revocación de los certificados (Jefe 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. **Responsable de la instalación, configuración y mantenimiento de los sistemas de la CA (Administrador de Sistemas)**:

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

d. **Responsable de la operación diaria de los sistemas de la CA, respaldo y recuperación de sistemas:**

Se encarga de las tareas de ejecución y revisión de las copias de seguridad del sistema. Asimismo debe velar para que se lleven a cabo las copias de seguridad locales y del traslado de las mismas de acuerdo con lo establecido en la política de seguridad.

Son responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible.

Encargados de la gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios.

e. **Funciones de auditoría interna para ejecutar la inspección y mantenimiento de los registros del sistema de la CA y de los registros de auditoría (Administrador de Auditoría):**

Son responsables de las tareas de ejecución y revisión de auditoría interna del sistema. Esta auditoría interna debe realizarse de acuerdo con las normas y criterios de auditoría establecidos en la CP y la presente CPS. Además cuenta con la capacidad de acceder a los registros del sistema.

f. **Funciones de gestión del ciclo de vida de claves criptográficas:**

Se distinguen los siguientes responsables para la gestión del ciclo de vida de las claves criptográficas:

- Oficial Criptográfico: Responsable de generar los usuarios que van a hacer uso de las claves del HSM. Participa en el backup y recuperación del HSM.
- Oficial de Activación: Responsable de activar las claves del HSM para que se pueda hacer uso de las mismas.
- Usuario: Es quien opera el sistema de gestión de certificados y el HSM, Oficial de Registro: Realiza funciones de registro, como la generación de certificados o la revocación de los mismos.

- Oficial de Generación de CRL: Encargado de generar y exportar en ficheros las CRLs emitidas por la CA. Además son responsables de activar los servicios de OCSP y asegurar la disponibilidad del CRL.

g. **Desarrollo de sistemas de la CA:**

Son encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones.

5.2.2 Número de personas requeridas por tarea

Se requiere un mínimo de dos personas con capacidad profesional suficiente para realizar las tareas.

5.2.3 Identificación y autenticación para cada rol

Para toda persona que aspira a 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
- 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

Además de lo estipulado en la CP, la asignación de personal garantizará que se cumplen las siguientes reglas de incompatibilidad:

- Un Administrador de HSM no puede ser Administrador de Auditoría
- Un Administrador de Sistemas no puede ser ni Coordinador de Seguridad ni Administrador de Auditoría
- Un Coordinador de Seguridad no puede ser Administrador de Sistemas ni Oficial de Registro, ni oficial Activación, ni Administrador de Auditoría
- Un Administrador de Auditoría incompatible con los demás roles

5.3 Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y autorización

Además de lo establecido en la CP, 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

Conforme lo estipulado en la CP.

5.3.3 Requerimientos de capacitación

Además de lo establecido en la CP, 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
- Procedimientos para la recuperación de la operación de la CA en caso de desastres.

5.3.4 Requerimientos y frecuencia de capacitación

Conforme lo estipulado en la CP.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

Conforme lo estipulado en la CP.

5.3.6 Sanciones para acciones no autorizadas

Conforme lo estipulado en la CP.

5.3.7 Requisitos de contratación a terceros

Además de lo establecido en la CP todo personal externo o consultores contratados deben firmar un acuerdo de confidencialidad como parte de los términos y condiciones de su incorporación.

5.3.8 Documentación suministrada al personal

Conforme lo estipulado en la CP.

5.4 Procedimiento de Registro de auditoría

5.4.1 Tipos de eventos registrados

En la CP se mencionan los tipos de eventos registrados.

5.4.2 Frecuencia de procesamiento del registro

Conforme lo estipulado en la CP.

5.4.3 Período de conservación del registro de auditoría

Conforme lo estipulado en la CP.

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

Conforme lo estipulado en la CP.

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

Conforme lo estipulado en la CP.

5.4.7 Notificación al sujeto que causa el evento

Conforme lo estipulado en la CP.

5.4.8 Evaluación de Vulnerabilidades

La evaluación de vulnerabilidades se debe llevar a cabo de forma periódica conforme lo establecido en la CP.

5.5 Archivos de registros

5.5.1 Tipos de registros archivados

Conforme lo estipulado en la CP.

5.5.2 Periodos de retención para archivos

Conforme lo estipulado en la CP.

5.5.3 Protección de archivos

Conforme lo estipulado en la CP.

5.5.4 Procedimientos de respaldo de archivo

Además de lo estipulado en la CP, la CA asume la obligación de:

- Mantener la integridad y confidencialidad del archivo que contiene los datos referentes a los certificados emitidos;
- Archivar los datos anteriormente citados de forma completa y confidencial;
- Mantener la privacidad de los datos de registro del suscriptor.

5.5.5 Requerimientos para sellado de tiempo de registros

No aplica

5.5.6 Sistema de recolección de archivo (interno o externo)

Conforme lo estipulado en la CP.

5.5.7 Procedimientos para obtener y verificar la información archivada

Esta verificación debe ser llevada a cabo por el Administrador de Auditoría que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la CA.

5.6 Cambio de clave

Conforme lo estipulado en la CP.

5.7 Recuperación de desastres y compromiso

5.7.1 Procedimiento para el manejo de incidente y compromiso

Conforme a lo estipulado en la CP.

5.7.2 Corrupción de datos, software y/o recursos computacionales

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

CA Raíz

En el caso de compromiso de la clave privada de la CA Raíz se procederá a la revocación inmediata de su certificado. Seguidamente, se generará y publicará la 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.

PSC

En el caso de compromiso de la clave privada, el PSC debe realizar como mínimo las siguientes acciones:

- Informar inmediatamente al MIC la situación y solicitar la revocación de su certificado
- Informar a todos sus suscriptores
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de este PSC ya no son válidos

5.7.4 Capacidad de continuidad del negocio después de un desastre

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,
- Procedimientos para asegurar la instalación de recuperación de Desastres durante el período de tiempo después de 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 tiempo objetivo para recuperar la funcionalidad del servicio de Producción crítico es no mayor que 24 horas.

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 Negocios formales donde son probados y evaluados procedimientos para tipos adicionales de escenarios (por ejemplo pandemias, inundaciones, apagones entre otros).

La CA debe adoptar pasos significativos para desarrollar, mantener y probar planes de recuperación de negocios confiables y los planes de la CA para un desastre o interrupción significativa del negocio debe ser consistente con las mejores prácticas internacionales establecidas.

La CA debe mantener hardware y respaldos de software de sistema e infraestructura en su recinto de recuperación de desastres. Además, las claves privadas de CA son respaldadas y mantenidas para fines de recuperación de desastre.

5.8 Terminación de una CA

Conforme lo estipulado en la CP.

6 CONTROLES TÉCNICOS DE SEGURIDAD

6.1 Generación e instalación del par de claves

La CA mantendrá controles para brindar seguridad razonable de que los pares de claves de la CA, se generan e instalan de acuerdo con el protocolo definido para la generación de claves.

6.1.1 Generación del par de claves

Además de lo estipulado en la CP, los pares de claves de la CA serán generados en módulos criptográficos de hardware que cumplan con las normas:

- CWA 14167-1 Requerimientos de Seguridad para Sistemas de confianza que administran certificados para firmas electrónicas (Security Requirements for trustworthy systems managing certificates for electronic signatures –part 1: System Security Requirements)
- CWA 14167-2 Requerimientos de Seguridad para Sistemas de confianza que administran certificados para firmas electrónicas (Security Requirements for trustworthy systems managing certificates for electronic signatures –part 2: Módulos criptográficos para operaciones de firma de PSC (cryptographic module for CSP Signing Operations – Protection Profile CMCSO-PP).

Toda CA debe elaborar un documento en el que especifiquen el procedimiento que indica los pasos de la Ceremonia de Creación de Claves y el mismo debe estar en conocimiento de las personas involucradas.

El módulo criptográfico de Hardware (HSM) debe cumplir con los siguientes requisitos:

- Permitir el gerenciamiento seguro del ciclo de claves asimétricas (generación asociación del certificado, backup, activación de uso y destrucción) para una CA.
- soportar los roles definidos en el punto 5.2.1 Roles de Confianza.

- generar registros de Auditoría como mínimo de: iniciación, cierre, creación de usuarios, remoción de usuarios.
- realizar auto test documentados con el objetivo de identificar un eventual compromiso del sistema. Como mínimo el auto test debe ocurrir con cada iniciación del HSM.
- permitir la configuración de activación de claves criptográficas a través de esquemas de secretos compartidos entre usuarios.
- soportar la configuración de autenticación de usuario basado en dos factores (conocimiento y posesión)
- permitir el backup de seguridad de claves criptográficas y parámetros críticos de seguridad mediante autorización utilizando un esquema de secreto compartido entre usuarios.
- La rutina de restauración de backup de claves criptográficas del HSM debe poseer un mecanismo de verificación de integridad del backup
- debe ser un equipamiento independiente. No está permitido el uso de placas criptográficas.

6.1.2 Entrega de la clave privada al suscriptor

La CA es responsable de la generación de su par de claves y por lo tanto del resguardo y custodia del mismo

La CA no tendrá acceso ni mantendrá copia de la clave privada de su suscriptor.

Cuando el par de claves de un usuario final es generado por éste, la entrega de la clave privada no es aplicable. En caso de que el par de claves del usuario final sea generado por el PSC en token de hardware o tarjetas inteligentes, tales dispositivos son distribuidos al usuario final utilizando un servicio de entrega segura y un embalaje que evidencie la intrusión. Los datos necesarios para activar el dispositivo son comunicados al usuario final mediante un proceso fuera de línea. La distribución de tales dispositivos es registrada por el PSC.

6.1.3 Entrega de la Clave Pública al emisor del Certificado

La clave pública generada bajo el control del PSC es entregada a la CA Raíz mediante el envío de una solicitud de firma de certificado (CSR) que concuerda con la especificación del PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

La clave pública generada bajo el control del usuario final es entregada al PSC mediante el envío de una solicitud de firma de certificado (CSR) que concuerda con la especificación del PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar. En el caso que el par de claves del usuario final sea generado por el PSC, este requisito no es aplicable.

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

La clave pública de la CA se encuentra incluida en el certificado de dicha CA. El certificado de la CA no se encuentra incluido en los certificados personales generados por el usuario final.

El certificado de la CA debe ser obtenido del repositorio que estará a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de comprobación.

6.1.5 Tamaño de la clave

Conforme lo estipulado en la CP.

6.1.6 Generación de parámetros de clave pública y verificación de calidad

Además de lo establecido en la CP, la clave pública de la CA está codificada de acuerdo con el RFC5280 y PKCS#1. El algoritmo de generación de clave es el RSA.

6.1.7 Propósitos de usos de clave (Campo key usage x509 v3)

Conforme lo estipulado en la CP.

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

6.2.1 Estándares y controles del Módulo criptográfico

Además de lo estipulado en la CP, los dispositivos empleados por la CA para la creación de las claves deben cumplir con la norma CWA 14167 partes 1 y 2 o por criterios de seguridad equivalentes.

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

- Inicialización del estado del módulo HSM.
- Creación de los dispositivos de administración y de operador.
- Generación de las claves de la CA.

6.2.2 Control multi-persona de clave privada

El control multi persona establecido en la CP, garantiza que nadie tenga el control de forma individual y completa de las actuaciones críticas.

6.2.3 Custodia de la clave privada

La custodia de la clave privada del certificado lo realiza los propios titulares de la misma.

6.2.4 Respaldo de la clave privada

Además de lo estipulado en la CP, la clave privada de respaldo debe estar almacenada y archivada en el módulo criptográfico de hardware (HSM) conforme la sección 6.1.1 de la presente CPS, compatible con el Fips 140-2 nivel 3 y al cual solo tienen acceso personal autorizado de la CA.

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

La clave privada de la CA puede ser exportada del módulo criptográfico únicamente para propósitos de respaldo, conforme a lo establecido en la CP y en el presente documento.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Conforme lo estipulado en la CP.

6.2.8 Método de activación de clave privada

Conforme lo estipulado en la CP.

6.2.9 Métodos de desactivación de la clave privada

Conforme lo estipulado en la CP.

6.2.10 Destrucción de clave privada

Además de lo establecido en la CP, el procedimiento de destrucción de clave privada, en el caso de la CA, debe estar documentado y realizado por personal con rol de confianza con control multipersona. La destrucción de la clave privada debe constar en los registros de auditoría.

6.2.11 Clasificación del Módulo criptográfico

Conforme lo estipulado en la CP.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La clave pública debe ser archivada por diez años desde el fin de su fecha de operatividad.

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

Conforme lo estipulado en la CP.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

La CA además de lo estipulado en la CP, deben elegir contraseñas seguras para proteger sus claves privadas de acuerdo a la siguiente guía:

- Que sean generadas por el usuario
- Tengan al menos ocho caracteres
- Deben tener un mínimo de cuatro caracteres distintos
- Tener al menos un carácter alfabético y uno numérico
- Tener al menos una letra minúscula y una mayúscula
- No contener demasiadas ocurrencias del mismo carácter
- No deben ser igual al nombre del perfil del operador
- No deben contener una porción larga del nombre del perfil del usuario
- No puede ser una secuencia de teclado que sea fácilmente adivinable (por ejemplo no puede ser la secuencia de **qwerty**)

6.4.2 Protección de los datos de activación

Solo el personal autorizado posee las tarjetas criptográficas con capacidad de activación de las claves privadas de la CA, asimismo, conoce los PINs necesarios para su utilización.

El número de identificación personal (PIN) es confidencial, personal e intransferible y es el parámetro que protege las claves privadas.

6.4.3 Otros aspectos de los datos de activación

Conforme lo estipulado en la CP.

6.5 Controles de seguridad del computador

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Además de lo estipulado en la CP, la CA debe asegurar que los sistemas que mantienen el software de producción y los archivos de datos son Sistemas de Confianza seguros ante el acceso no autorizado. Además, debe limitar el acceso a los servidores de producción a aquellos individuos con un motivo válido para tal acceso, todos estos deben ser registrados.

La red de producción de la CA debe estar separada lógicamente de otros componentes. La CA debe utilizar cortafuegos para proteger la red de producción contra intromisiones internas y externas y limitar la naturaleza y fuente de actividades de red que pueden acceder a sistemas de producción.

El acceso directo a las bases de datos de la CA que soportan las operaciones de la misma está limitado a personas autorizadas.

6.5.2 Clasificación de la seguridad del computador

Conforme 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

La CA debe realizar controles para proporcionar seguridad al dispositivo que genera las claves. Para evitar posibles incidencias en los sistemas, se establecen los siguientes controles:

- El módulo criptográfico de hardware de generación de claves debe ser probado antes de su puesta a producción
- La generación de claves se produce dentro de los módulos criptográficos requeridos.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de la ceremonia de generación de claves.

6.7 Controles de seguridad de red

Conforme lo estipulado en la CP.

6.8 Sellado de tiempo (Time-stamping)

No aplica

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

7.1.2.1 Key Usage

Conforme lo estipulado en la CP.

7.1.2.2 Extensión de política de certificados

Conforme lo estipulado en la CP.

7.1.2.3 Nombre alternativo del sujeto

Conforme lo estipulado en la CP.

7.1.2.4 Restricciones básicas

Conforme lo estipulado en la CP.

7.1.2.5 Uso extendido de la clave

Conforme lo estipulado en la CP.

7.1.2.6 Puntos de distribución de los CRL

Conforme lo estipulado en la CP.

7.1.2.7 Identificador de clave de Autoridad

Conforme lo estipulado en la CP.

7.1.2.8 Identificador de la clave del sujeto

Conforme lo estipulado en la CP.

7.1.2.9 QcStatements

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.

7.2 Perfil de la CRL

Conforme lo estipulado en la CP.

7.2.1 Número (s) de versión

Conforme lo estipulado en la CP.

7.2.2 CRL y extensiones de entradas de CRL

7.2.2.1 Número CRL (CRL Number)

Conforme lo estipulado en la CP.

7.2.2.2 Identificador de clave de Autoridad

Conforme lo estipulado en la CP.

7.2.2.3 Puntos de distribución de las CRL

Conforme lo estipulado en la CP.

7.3 Perfil de OCSP

Conforme lo estipulado en la CP.

7.3.1 Número (s) de versión

Conforme lo estipulado en la CP.

7.3.2 Extensiones de OCSP

Sin estipulaciones.

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Además de lo establecido en la CP, el sistema de Auditoría de la CA debe tener en cuenta cuanto menos las siguientes medidas:

1. Realizar de forma periódica comprobaciones regulares de la seguridad, con el fin verificar la conformidad con los estándares establecidos.

2. Llevar a cabo una completa gestión de los sucesos de seguridad, con el fin de garantizar su detección, resolución y optimización.

3. Mantener los contactos y relaciones apropiadas con grupos de especial interés en materia de seguridad, como especialistas, foros de seguridad y asociaciones profesionales relacionadas con la seguridad de la información.

4. Planificar adecuadamente el mantenimiento y evolución de los sistemas, con el fin de garantizar en todo momento un rendimiento adecuado y un servicio que cumpla con todas las garantías, las expectativas de los usuarios

8.1 Frecuencia o circunstancias de evaluación

Conforme lo estipulado en la CP

8.2 Identidad/calidades del evaluador

Para cada control y según el área sometida a revisión, el personal encargado en llevar a cabo esta operación, debe contar con la experiencia necesaria, demostrar dominio de la tecnología de infraestructura de clave pública, herramientas y técnicas de seguridad de la información y auditoría de seguridad.

8.3 Relación del evaluador con la entidad evaluada

Conforme lo estipulado en la CP.

8.4 Aspectos cubiertos por la evaluación

Además de lo establecido en la CP serán objeto de Auditoría:

- 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, etc.

Los detalles de cómo se lleva a cabo la auditoría de cada uno de los elementos previstos en la CP o CPS deben ser especificados en el Manual de Procedimiento de Auditoría.

8.5 Acciones tomadas como resultado de una deficiencia

Conforme lo estipulado en la CP.

8.6 Comunicación de resultados

Conforme lo estipulado en la CP.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

La CA Raíz, no se encuentra sujeta al pago de tarifas o aranceles sin embargo, el PSC, se encuentra obligado a cumplir con las tasas y aranceles impuestos por el MIC.

El PSC deberá comunicar al interesado en adquirir un certificado digital de todos los costos que deberá asumir para la obtención del certificado.

9.1.1 Tarifas de emisión y administración de certificados

Conforme lo estipulado en la CP.

9.1.2 Tarifas de acceso a certificados

El acceso a certificados es un servicio gratuito.

9.1.3 Tarifas de acceso a información del estado o revocación

El acceso a la información de estado o revocación a través de consulta de la CRL disponible en el sitio de internet es gratuito. El PSC puede cobrar una tarifa por servicios de OCSP u otros servicios de valor agregado sobre información de estado y revocación, los costos deben establecerse en su CP y publicarse en el sitio de internet.

9.1.4 Tarifas por otros servicios

Conforme lo estipulado en la CP.

9.1.5 Políticas de reembolso

Conforme lo estipulado en la CP.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

Conforme lo estipula en la CP.

9.2.2 Otros activos

Conforme lo estipulado en la CP.

9.2.3 Cobertura de seguro o garantía para usuarios finales

Conforme lo estipulado en la CP.

9.3 Confidencialidad de la información comercial

La CA, debe comprometerse a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como integrante de la PKI Paraguay. No obstante, la CA se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como tal. En este caso, los empleados y/o consultores deben ser informados sobre las obligaciones de confidencialidad, las que

deben ser establecidas en sus respectivos contratos. Estas obligaciones no se aplican si la información calificada como "confidencial" es requerida por los Tribunales, órganos competentes o impuestos por una ley.

9.3.1 Alcance de la información confidencial

Conforme lo estipulado en la CP.

9.3.2 Información no contenida en el alcance de información confidencial

Además de lo estipulado en la CP, se considera información no confidencial:

- Contenido de los certificados emitidos
- La clave pública de la CA
- Las versiones de la CP y CPS
- Toda otra información identificada como "Pública".

9.4 Privacidad de información personal

9.4.1 Plan de Privacidad

Conforme lo estipulado en la CP.

9.4.2 Información tratada como privada

Conforme lo estipulado en la CP.

9.4.3 Información que no es considerada como privada

Conforme lo estipulado en la CP.

9.4.4 Responsabilidad para proteger información privada

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

Conforme lo estipulado en la CP.

9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo

Conforme lo estipulado en la CP.

9.4.7 Otras circunstancias de divulgación de información

Conforme lo estipulado en la CP.

9.5 Derecho de Propiedad intelectual

La CA debe mantener en forma exclusiva todos los derechos de propiedad intelectual, con respecto a la Declaración de Prácticas, aplicaciones pertenecientes a ella, certificados emitidos y CRL.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

Además de lo estipulado en la CP, la CA debe garantizar:

CA Raíz

- 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;

- 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.

PSC

- Tener conocimiento de los pasos necesarios para la habilitación ante el MIC;
- Actuar con diligencia para evitar el uso no autorizado de su Firma Digital;
- 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 Firma Digital ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello;
- Elaborar su propia CPS y CP, que deberán ser acordes a las de la AC Raiz.

9.6.2 Representaciones y garantías de la RA

Además de lo estipulado en la CP, la CA en su función de Registro debe cumplir con las siguientes obligaciones:

- Realizar sus operaciones de conformidad con esta CPS y la CP;
- Comprobar exhaustivamente la identidad del suscriptor para lo que se requerirá la presencia física del mismo, o de su representante legal cuando aplique, y los documentos necesarios que se describen en la normativa vigente;
- No almacenar ni copiar datos de creación de firma del titular del certificado;

- Informar, antes de la emisión del certificado, al solicitante, sobre las obligaciones que asume;
- En el caso que el solicitante sea un PSC, informar antes de la 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 DPC y la PC 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/certificado notificar al solicitante;
- En el caso del rechazo de una solicitud de habilitación/certificado, 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

Además de lo estipulado en la CP, el suscriptor debe:

- Conocer y aceptar las condiciones de utilización de los certificados, tal como lo establece esta CPS, y la CP;

- Limitar y adecuar el uso del certificado a propósitos lícitos y acordes con los usos permitidos por la presente CPS y la CP;
- Poner el cuidado y medios necesarios para garantizar la custodia de su clave privada, evitando su pérdida, divulgación, modificación o uso no autorizado;
- Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado y demás causales de revocación establecidas en la norma;
- Cesar inmediatamente el uso del certificado y la clave privada relacionada después de la expiración del certificado;
- Cualquier otra obligación que derive de la normativa vigente.

9.6.4 Representaciones y garantías de las partes que confían

Es obligación de las partes que confían en los certificados emitidos en el marco de la PKI Paraguay:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, de conformidad con lo expresado en las extensiones de los certificados y la CP pertinente;
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos;
- Asumir su responsabilidad en la correcta verificación de las firmas digitales;
- Asumir su responsabilidad en la comprobación de la validez o revocación de los certificados en que confía;
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas;

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

9.6.5 Representaciones y garantías de otros participantes

Sin estipulaciones.

9.7 Exención de garantía

Conforme lo estipulado en la CP.

9.8 Limitaciones de responsabilidad legal

Dentro de los límites permitidos por la normativa vigente que rige la materia, en el Acuerdo de Suscriptores se establecerá y limitará la responsabilidad tanto de suscriptores como de la propia CA. Las limitaciones de responsabilidad deberán incluir una exclusión de daños indirectos, especiales, incidentales y derivados.

9.9 Indemnizaciones

Además de lo estipulado en la CP, se establecen las causas de indemnización de los suscriptores a la CA:

- Falsedad o tergiversación de hecho por el Suscriptor en la Solicitud de Certificado
- La no revelación de un hecho sustancial en la Solicitud de Certificado, si la falsedad u omisión es consecuencia de negligencia o con la intención de engañar a cualquiera de las partes
- Faltas del Suscriptor para la protección de su clave privada, para utilizar un sistema seguro o para tomar, en cualquier otro caso las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de su clave privada, o

- El uso por parte del Suscriptor de un nombre (incluyendo, sin limitaciones dentro de un nombre común, un nombre de dominio o una dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de un tercero.

El Acuerdo de Suscriptor aplicable puede incluir obligaciones de indemnización adicionales.

9.10 Plazo y finalización

9.10.1 Plazo

La CPS de la CA Raíz empieza a ser efectiva una vez aprobado el contenido del documento por Resolución Ministerial y los nuevos certificados deben ser emitidos cumpliendo las políticas y procedimientos determinados en la nueva versión de la CP y la CPS. La CPS del PSC empieza a ser efectiva una vez publicada en su sitio de internet, previa aprobación del MIC, y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la CP y la CPS.

9.10.2 Finalización

La CPS 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 declaración seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Declaración de Prácticas contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

9.11 Notificación individual y comunicaciones con participantes

Conforme lo estipulado en la CP.

9.12 Enmiendas

9.12.1 Procedimientos para enmiendas

Conforme lo estipulado en la CP.

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

Dentro de los límites de la normativa, el Acuerdo de Suscriptores deberá contener una cláusula de resolución de disputas. La CA se somete voluntariamente para la solución de cualquier cuestión litigiosa que pudiera surgir por el ejercicio de su actividad, no obstante en el caso de que la alguna de las partes contrarias a ella no acepte el procedimiento extrajudicial, todas las partes deben someterse expresamente a los Juzgados y Tribunales de la ciudad capital con renuncia a su propia jurisdicción si fuese otra.

9.14 Normativa aplicable

Conforme lo estipulado en la CP.

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 esta Declaración se mantendrán vigentes.

9.16.4 Aplicación (Honorarios de Abogados y renuncia de derechos)

No aplica

9.16.5 Fuerza mayor

Conforme lo estipulado en la CP.

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.

La CPS del PSC, debe guardar concordancia con las disposiciones de la presente Declaración de Prácticas.

10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de la Declaración de Prácticas de certificación:

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