code100 S.A.
SERVICIOS DE CERTIFICACION DIGITAL

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

VERSIÓN 4.0

CONTROL DOCUMENTAL

DOCUMENTO	
TÍTULO: **DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN**	NOMBRE DEL ARCHIVO: CODE100 DECLARACIÓN DE PRACTICAS V4.0.DOCX
CÓDIGO: **CODE100 DECLARACIÓN DE PRACTICAS V4.0**	SOPORTE LÓGICO: HTTPS://WWW.CODE100.COM.PY/FIRMA-DIGITAL/INDEX.PHP
FECHA: 10/09/2019	UBICACIÓN FÍSICA: CODE100 S.A.
VERSIÓN: 4.0	

REGISTRO DE CAMBIOS		
VERSIÓN	FECHA	MOTIVO DE CAMBIO
VERSIÓN 1.0	01/04/2014	APROBACIÓN PARA PRESENTACIÓN
VERSIÓN 1.2	22/12/2014	APROBACIÓN PARA PRESENTACIÓN
VERSIÓN 2.O	07/02/2017	APROBACIÓN PARA PRESENTACIÓN
VERSIÓN 3.O	28/08/2018	APROBACIÓN PARA PRESENTACIÓN
VERSIÓN 4.O	10/09/2019	APROBACIÓN PARA PRESENTACIÓN

DISTRIBUCIÓN DEL DOCUMENTO	
Nombre	Área
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
CODE100 S.A.	Directorio CODE100
Documento Público	www.code100.com.py

CONTROL DEL DOCUMENTO		
Preparado por:	**Revisado por:**	**Aceptado por:**
Celia Rodríguez	Pablo Benítez	Directivo CODE100 S.A.

INDICE

Índice

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

CODE100 S.A. en su calidad de Prestador de Servicios de Certificación (en adelante "PSC") brinda los servicios de certificación digital según lo establecido por la Ley Nro. 4017/10, Nro. 4610/12, Decreto Reglamentario Nro. 7369/11.

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

El Ministerio de Industria y Comercio como ente regulador debe:

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

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

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

El presente documento es la **Declaración de Prácticas de Certificación de CODE100 S. A**. (en adelante "CPS") con habilitación otorgada por el Ministerio Industria y Comercio (MIC), en su carácter de Autoridad de Aplicación de la Infraestructura de Clave Pública del Paraguay, aprobada por el Directorio y personal autorizado de CODE100 S.A., acorde a la CP de la Infraestructura de Clave Pública del Paraguay.

Esta CP es aplicable a:

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

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	Declaración de Prácticas de Certificación de CODE100 S.A.
Versión:	4.0
Fecha de aprobación:	09/09/2019
Ubicación de la CPS:	http://www.code100.com.py/firma-digital/

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. Así mismo, efectúan la revocación de los mencionados certificados y la generación de claves públicas y privadas, cuando así lo establecen sus prácticas y políticas. Esto incluye a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz)

La CA Raíz es administrada por la AA y sus funciones están estipuladas en su CP, CPS y en la normativa vigente. La CA Raíz emite certificados a los PSC.

- Prestador de Servicios de Certificación (PSC)

CODE100 S.A presta servicios de certificación digital habiendo sido habilitado por el MIC luego de presentar la Solicitud de Habilitación ajustándose al procedimiento establecido para el efecto. El PSC emite certificados digitales a los usuarios finales.

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, den 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 Agente de Registro Validador quien 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 original del Acuerdo con Suscriptores y posteriormente entregar el certificado solicitado.

Los datos referentes a las RA habilitadas por CODE100 S.A. se encuentran en la dirección de página web (URL) http://www.code100.com.py/autoridad-de-registro

El PSC CODE100 S.A. mantiene publicada en el sitio las siguientes informaciones actualizadas:

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

1.3.3. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

Las PSS son entidades externas a las que recurre la CA o la RA para desempeñar actividades descritas en esta CP o en una CPS y se clasifican en tres categorías, conforme al tipo de servicio prestado:

a) Disponibilización de infraestructura física y lógica;

b) Disponibilización de recursos humanos especializados;

c) Disponibilización de infraestructura física y lógica y de recursos humanos especializados.

Los PSS de CODE100 S.A. se publicarán en el sitio:

http://www.code100.com.py/firma-digital/prestadores-soporte

1.3.4. SUSCRIPTORES

En relación con CODE100 S.A., 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.

1.3.5. 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.

1.3.6. OTROS PARTICIPANTES

Sin estipulaciones.

1.4 USO DEL CERTIFICADO

1.4.1 USOS APROPIADOS DEL CERTIFICADO

Las Políticas de Certificación del PSC CODE100 S.A. correspondientes a cada tipo de certificado que emita son las que determinan los usos apropiados que debe darse a cada certificado.

A continuación se describen los usos apropiados del Certificado de la CA raíz y del PSC CODE100 S.A.

TIPO	**DESCRIPCION DE USO APROPIADO**
Certificado de CA Raíz	Firma de Certificado a PSC. Firma de CRL de PSC. • Firma de Certificado (Certificate Signing). • Firma CRL sin conexión (Off line CRL Signing).
Certificado del PSC CODE100 S.A.	Firma de Certificado a sus suscriptores. Firma de CRL de sus suscriptores. • Firma de Certificado (Certificate Signing). • Firma de CRL (CRL Signing). • Firma CRL sin conexión (Off line CRL Signing).

• **Firma de Certificado** (Certificate Signing): se usa en caso de 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 Signin Lg) 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. Las claves privadas o secretas, es decir, para la clave de transporte. Por ejemplo, cuando una clave pública RSA es utilizada para encriptar la clave simétrica o una clave privada asimétrica;

• **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 de CODE100 S.A. determina las limitaciones y restricciones en el uso de los certificados. No es objetivo de esta CPS la determinación de dichas limitaciones y restricciones.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: CODE100 S.A.

Dirección: Benjamín Constant 973, Edificio Arasá 2, Oficina 12

Teléfono: *(+59521) 445 601/2*

Dirección de correo electrónico: info@code100.com.py

Página Web: www.code100.com.py

1.5.2. PERSONA DE CONTACTO

Nombre: Representante Legal de CODE100 S.A.

Dirección: Arellano 1225, Sajonia Asunción Paraguay

Teléfono: (+595) (981) 387 008

Dirección de correo electrónico: info@code100.com.py

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA POLÍTICA

El Director General de Firma Digital y Comercio Electrónico, será el encargado de determinar la adecuación de la presente Declaración de Prácticas de Certificación (CPS) de la PKI y la del CODE100 S. A.

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CPS

El MIC aprobará el contenido de la presente CPS y sus posteriores enmiendas o modificaciones.

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 DEFINICIONES

Acuerdo de Suscriptores: es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita de las partes intervinientes.

Agente de Registro Validador: Persona responsable de la ejecución de actividades relacionadas con la RA, que realiza la validación de la identidad de quien solicita un certificado digital.

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

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

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

Autoridad de Aplicación (AA): se designa al Ministerio de Industria y Comercio como órgano regulador competente 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". Ejerce funciones a través de su unidad administrativa, la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio.

Autoridad de Certificación (CA): entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI Paraguay, son Autoridades de Certificación, la CA Raíz del Paraguay y el PSC.

Autoridad Certificadora Raíz o Autoridad de Certificación Raíz (CA Raíz): es el órgano técnico dentro de la PKI, cuya función principal es habilitar

al PSC y emitir a éste, el certificado digital correspondiente. Posee un certificado auto firmado y es a partir de í, donde comienza la cadena de confianza.

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

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

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

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

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

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

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

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

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

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

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

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

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

Datos de activación: valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

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

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

Emisión: comprende la generación del certificado, cuyo proceso es una función de la CA.

Emisor del certificado: organización cuyo nombre aparece en el campo emisor de un certificado. Estándares Técnicos Internacionales: requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Firma Digital: es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación,

verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

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

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

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

Identificador de Objeto (OID): los identificadores de objeto son un sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.

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

Integridad: característica que indica que un mensaje de datos o un 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 diferente del titular, que decide aceptar y confiar en un certificado emitido bajo la jerarquía de la PKI Paraguay.

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

Período 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.

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

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

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

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

Ruta del certificado: secuencia ordenada de certificados de entidades que, junto a la clave pública de la entidad inicial en la ruta, puede ser procesada para obtener la clave pública de la entidad final en la ruta. **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.

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

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

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

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

Validez de la firma: aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado. Verificación de la firma: determinación y validación de: a) que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

X. 500: estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511. X.518, X.519, X.520, X.521, X.525.

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

1.6.2 ACRÓNIMOS

Tabla Nº1 - Acrónimos

Acrónimos	Descripción
C	País (del inglés, Country)
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority)
CAI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés Certificate Authority Intermediate)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cedula de Identidad
CN	Nombre Común (del inglés, Common Name)
CP	Política de Certificación (CP por sus siglas en inglés Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement)
CRL	Lista de Certificados Revocados (CRL por sus siglas en inglés Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés Certificate Signing Request)

DGFD&CE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministro de Comercio
DNS	Servicio de nombre de dominio (DNS por sus siglas en inglés Domain Name Server
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 su sigla en inglés Hardware Security module)
ISO	Organización Internacional para la Estandarización (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 Standarization Sector)
MIC	Ministerio de Industria y Comercio
O	Organización (del inglés Organization)
OCSP	Servicio de Validación de certificado 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 Publica (PKI por su sigla en inglés Public Key Infraestructure)
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)
TLS	Transport Layer Security (seguridad de la capa de transporte)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés Uninterruptible Power Supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés Uniform Resource Locator)

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

2. RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

2.1. REPOSITORIOS

El PSC CODE100 S.A. dispone del siguiente sitio de internet como repositorio público de información: https://www.code100.com.py y cuyo acceso será gratuito e irrestricto. El mismo está disponible en un 99,5% anual, durante 24 horas al día, 7 días a la semana. El acceso se realiza vía el protocolo HTTPS.

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El PSC CODE100 S. A. garantiza que todos los certificados de la cadena de confianza estén publicados y disponibles en el sitio principal de internet.

El repositorio del PSC CODE100 S. A. está disponible durante 24 horas al día, 7 días a la semana. Consiste en un servicio Web de acceso libre. Dicho repositorio no contiene ninguna información de naturaleza confidencial. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99% anual, un tiempo programado de inactividad máximo de 0,5% anual.

EL PSC de CODE100 S.A. mantiene un repositorio en su sitio principal de internet que permite a las partes que confían verificar en línea la revocación de un certificado y cualquier otra información necesaria para validar el estado del mismo.

EL PSC CODE100 S.A. mantiene publicada, entre otros aspectos la versión actualizada de:

Lista de Certificados Revocados	http://ca1.code100.com.py/firma-digital/crl/CA-CODE100.crl
Servicio OCSP	http://ca1.code100.com.py/ocsp http://ca2.code100.com.py/ocsp

CA Raíz del Paraguay	http://www.code100.com.py/firma-digital/crt/ac_raiz_py_sha256.crt
Certificado de la CA CODE100 S.A.	https://ca1.code100.com.py/firma-digital/cer/ca-code100.crt
CPS	https://www.code100.com.py/firma-digital/
Política de Certificación F1	https://www.code100.com.py/firma-digital/
Política de Certificación F2	https://www.code100.com.py/firma-digital/
Consulta de Certificados Emitidos	https://ca1.code100.com.py/ServicioDescargas.aspx
Acuerdo con Suscriptores	https://www.code100.com.py/firma-digital/
PSS vinculados	http://www.code100.com.py/firma-digital/prestadores-soporte
Información de RA delegadas	https://www.code100.com.py/autoridad-de-registro

Además, se publican Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay; las resoluciones que habilitan, suspenden o revocan al PSC; y la información relevante del resultado de la última auditoría que hubiere sido objeto.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Las enmiendas o modificaciones de la CPS se publicarán de acuerdo con lo establecido en el punto 9.12 de este documento. Las actualizaciones del Acuerdo de Suscriptores serán publicadas cuando sufran modificaciones.

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

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

2.4 CONTROLES DE ACCESO

CODE100 S.A. implementa 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

CODE100 S.A. describe los requisitos y procedimientos utilizados por la RA vinculadas al PSC responsable de llevar a cabo los siguientes procesos:

a) **Validación de solicitud de certificado**: realizada mediante presencia física del interesado presentando los documentos de identificación indicados en los ítems 3.2.2, 3.2.3 y 3.2.4 comprendiendo las siguientes etapas:

i) **Confirmación de identidad de la persona física**: comprobar que la persona que se presenta como titular interesado en un certificado de persona física sea realmente aquella cuyos datos constan en la documentación presentada. Está prohibido cualquier especie de representación para este fin. En caso de persona jurídica, comprobar que la persona física que se presenta como representante es realmente aquella cuyos datos constan en la documentación presentada. El responsable de uso del certificado digital para persona jurídica debe comparecer presencialmente. Está prohibido cualquier especie de representación para este fin.

ii) **Confirmación de la identidad de una persona jurídica**: comprobar que los documentos presentados refieren efectivamente a la persona jurídica, titular del certificado y de que la persona que se presenta como representante legal de la persona jurídica realmente posea tal atribución; y

iii) **Autorización de emisión del certificado**: Confirmar los datos de solicitud de certificado con el conjunto de los documentos presentados y autorizar la expedición del certificado en el sistema del PSC;

b) **Verificación de la solicitud de certificado**: confirmar la validación realizada, señalando que debe ser ejecutado, obligatoriamente:

i) Por el agente de registro distinto al que ejecuto la tarea en la etapa de validación;

ii) En una de las instalaciones técnicas de la RA debidamente autorizada por el PSC al cual está vinculada;

iii) Únicamente después de la recepción, en la instalación técnica de la RA, de las copias de las documentaciones presentadas en la etapa de validación; y

iv) Antes del inicio de la validez del certificado, debiendo ser revocado inmediatamente en el caso que la validación no se haya realizado antes del inicio de su validez.

El proceso de validación de la identidad podrá ser realizado por el agente de registro validador fuera del ambiente físico de la RA, siempre que haya utilizado un ambiente computacional auditable y debidamente registrado en el inventario de hardware y software de la RA.

Todas las etapas de los procesos de validación y verificación de la solicitud de certificados son registradas y firmadas por los ejecutantes. Estos registros se realizan a los efectos de permitir la reconstrucción completa de los procesos ejecutados, con fines de auditoria.

Se mantiene un archivo con las copias de todos los documentos utilizados para la confirmación de la identidad de una organización y/o individuo. Las copias se mantienen en papel o digitalizadas, sujeto a las condiciones expuestas en este documento.

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

El tipo de nombre admitido para los titulares de los certificados emitidos conforme a la presente CPS son el Nombre Distintivo (Distinguished Name) según lo establecido en el estándar ITU X.500, direcciones de correo electrónico, dirección de página web (URL), u otra información que permita la identificación única del titular.

3.1.2 NECESIDAD DE NOMBRES SIGNIFICATIVOS

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

3.1.3 ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

No se admite el anonimato en los certificados emitido por un PSC. Asimismo, el seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Certificado de PSC, Certificado de Persona Jurídica para firma digital o cifrado.

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

Tipo de Documento	Prefijo	Formato
Cédula Tributaria – RUC	RUC	RUC99999999-9

Certificado de Persona física para firma digital o cifrado

La Cédula de identidad es expedida por el Departamento de Identificaciones de la Policía Nacional, y debe cumplir el siguiente formato:

Tipo de Documento	Prefijo	Formato
Cédula de identidad CI	CI	CI9999999

Certificado de máquina o aplicación

Tipo de Documento	Prefijo	Formato
Cédula de identidad CI	MCI	CI9999999
Cédula tributaria – RUC	MRUC	RUC99999999-9

3.1.5 UNICIDAD DE LOS NOMBRES

El "Distinguished Name" (DN) del suscriptor, deberá ser único para cada titular del certificado, en el ámbito de la PKI de CODE100 S.A. Números y letras adicionales podrán ser incluidos al nombre de cada entidad para asegurar la unicidad del campo.

3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

CODE100 S.A. se reserva el derecho de tomar todas las decisiones en el caso de que haya conflicto derivado de los nombres iguales entre varios solicitantes de certificados.

También, durante el proceso de verificación de identidad, corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico.

CODE100 S.A. tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

El proceso de comprobación de identidad de la persona física o jurídica cuyos datos se incluyen en un certificado digital tiene como objetivo garantizar que el suscriptor sea la persona identificada en la solicitud del certificado, y que la información que se incluya en el certificado sea exacta. En principio, la exactitud y veracidad de la información proporcionada por el suscriptor es atribuida al mismo, sin perjuicio de la respectiva comprobación por parte del PSC CODE100 S.A.

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

El solicitante del certificado debe demostrar que posee la clave privada correspondiente a la clave pública que deberá ser listada en el Certificado.

La posesión de la clave privada, correspondiente a la clave pública para la que se solicita que se genere el certificado, quedará probada mediante el envío de la solicitud de certificado (CSR) en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por la Autoridad de Aplicación, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

El titular del Certificado de Persona Jurídica será la persona física, designada por la organización como responsable del certificado, que será el titular de la clave privada.

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.

CODE100 S.A. como mínimo exigirá la presentación de los siguientes documentos respaldatorios:

i. Si la entidad es publica:

   a. Copia simple de la Ley o Carta Orgánica que crea o autoriza su creación;

b. Documento que acredite la representación legal de la máxima autoridad; y

c. Número de registro único del contribuyente (RUC), en caso de que la entidad pública sea sujeto tributario.

ii. Si la entidad es privada:

a. Copia autenticada del documento de constitución de la sociedad;

b. Copia autenticada de acta de la última asamblea Ordinaria y Extraordinaria;

c. Copia autenticada del Acta de la última sesión;

d. Prueba de la inscripción en el registro nacional de personas jurídicas;

e. Certificado de cumplimiento tributario;

f. Número de registro único del contribuyente (RUC).

La confirmación de la identidad de el/los representante/s legal/es de la persona jurídica y del responsable del uso del certificado, se hará mediante la presentación de los documentos exigidos en el Ítem 3.2.3, con la presencia física de estos y la firma del documento de solicitud de certificado que trata el ítem 4.1.

La información obligatoria contenida en los campos del certificado expedido a una persona jurídica, debe coincidir exactamente con la información contenida en los siguientes documentos:

a) Nombre de la razón social según documento constituido, sin abreviaturas, en el campo Subject, como parte del Common Name, que compone parte del Distinguished Name;

b) Número de registro único del contribuyente (RUC) según la cédula tributaria en el campo Subject, como parte del SerialNumber, que compone parte del Distinguished Name;

c) Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo Subject Alternative Name OID=2.5.4.3

d) Número de cedula de Identidad Policial de la persona física responsable del certificado según documento de identidad, en el campo Subject Alternative Name OID=2.5.4.3

La RA vinculada al PSC debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes. Si hay diferencias en

relación con los datos del documento de identidad de la persona física, la expedición del certificado digital debe ser suspendida y el solicitante debe regularizar su situación ante el organismo competente.

Cada CP puede definir como obligatoria llenar otros campos.

Además el titular del certificado, a su criterio y mediante una declaración explicita en el documento de solicitud de certificado, puede solicitar llenar los campos con las siguientes informaciones:

a) El correo del titular del certificado; y

b) El cargo que ocupa en la organización el responsable del certificado.

Para ello, el titular deberá presentar la documentación que respalde la información, caso por ello, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copia de todos los documentos utilizados.

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.

Esta comprobación se realiza mediante la presencia física de la persona, sobre la base de los documentos de identificación legalmente aceptados y cotejados con registros oficiales.

Para la comprobación de la identidad de la persona física se deben presentar la siguiente documentación vigente en su versión original:

a) Cédula de Identidad Policial Paraguaya;

b) Otro documento oficial emitido por un Ente del Gobierno, pudiendo ser:

b.1) Licencia de conducir del solicitante.

b.2) Pasaporte

b.3) Certificado de Antecedentes Penales

b.4) Certificado de Antecedentes Judiciales

b.5) Certificado de Nacimiento, entre otros.

La información obligatoria contenida en los campos del certificado expedido a una persona física debe coincidir exactamente con la información contenida en los siguientes documentos:

a) Nombre completo de la persona física titular del certificado, según el documento de identidad, en el campo Subject, como parte del Common Name, que compone parte del Distinguished Name; y

b) Número de Cédula de Identidad Policial de la persona física, según documento de identidad, en el campo Subject, como parte del SerialNumber, que compone parte del Distinguished Name.

La RA de CODE100 S.A. debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes. Si hay diferencias en relación con los datos del documento de identidad, la expedición del certificado digital debe ser suspendida y el solicitante debe regularizar su situación ante el organismo competente.

Cada CP puede definir como obligatoria llenar otros campos.

Además, el titular del certificado, a su criterio y mediante una declaración explicita en el documento de solicitud de certificado, puede solicitar llenar los campos las siguientes informaciones:

a) El correo del titular del certificado;

b) El nombre de la organización en el que presta servicio el titular del certificado.

c) El nombre de la unidad de la organización en el que presta servicio el titular del certificado;

d) El número de cédula tributaria correspondiente al titular del certificado; y

e) El cargo o título del titular del certificado.

Para ello, el titular deberá presentar la documentación que respalde la información, caso por caso, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copias de todos los documentos utilizados.

3.2.4 AUTENTICACIÓN DE IDENTIDAD DE UNA MÁQUINA O APLICACIÓN

En el caso de los certificados expedidos para una maquina o aplicación, el titular es la persona física o jurídica que solicita el certificado. En el caso de que el solicitante sea una persona jurídica, se deberá indicar al responsable del certificado, que será el titular de la clave privada.

Si el titular del certificado es una persona física, se deberá confirmar su identidad según lo estipulado en el ítem 3.2.3 y la firma del documento de solicitud de certificado que trata el ítem 4.1.

Si el titular del certificado es una persona jurídica, se deberá confirmar su identidad según lo estipulado en el ítem 3.2.2 y la firma del documento de solicitud de certificado que trata el ítem 4.1.

Procedimientos para la identificación de una maquina o aplicación:

a) Para emisión de certificados de máquinas que se utilizan como servidores, la solicitud debe contener el nombre del servidor y el número de serie del equipamiento.

b) Para certificados de máquina o aplicación que utilizar URL en el campo Common Name, se debe comprobar si el solicitante del certificado tiene el registro del nombre de dominio por el órgano competente, o tenga el permiso del propietario del dominio para utilizar ese nombre. En este caso, se debe presentar la documentación correspondiente (autorización o similar) firmado por el titular del dominio.

La información obligatoria contenida en los campos del certificado expedido a un dispositivo o aplicación debe coincidir exactamente con la información contenida en los siguientes documentos:

a) URL o nombre de la aplicación, en el campo Subject, como parte del Common Name, que compone el Distinguished Name;

b) En caso de que el titular sea una persona jurídica:

b.1) Número de registro único del contribuyente (RUC) de la persona jurídica según la cedula tributaria en el campo Subject, como parte del SerialNumber, que compone parte del Distinguished Name;

b.2) Nombre de la razón social de la persona jurídica según documento constitutivo, en el campo Subject Alternative Name OID:2.5.4.10;

b.3) Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo Subject Alternative Name OID:2.5.4.3

b.4) Número de cedula de identidad policial de la persona física responsable del certificado según documento de identidad, en el campo Subject Alternative OID:2.5.4.5

c) En el caso que el titular sea una persona física:

c.1) Número de cédula de identidad policial de la persona física, según documento de identidad, en el campo Subject, como parte del SerialNumber, que compone parte del Distinguished Name;

c.2) Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo Subject Alternative Name OID:2.5.4.3

Además, el titular del certificado, a su criterio y mediante una declaración explícita en el documento de solicitud de certificado, puede solicitar llenar los campos con las siguientes informaciones:

a) El correo del responsable del certificado;

b) El cargo o título del responsable del certificado en caso de ser persona jurídica.

Para ello, el titular deberá presentar la documentación que respalde la información, caso por caso, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copia de todos los documentos utilizados.

3.2.5 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

No aplica.

3.2.6. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

CODE100 S.A. Determinará si el solicitante se encuentra apto para solicitar un tipo de certificado específico. Además, debe validar que el solicitante no posea impedimentos legales.

En el caso de Certificados de Personas Físicas, validará:

- Nombre y documento de identidad
- Mayoría de edad.

En el caso que el solicitante sea Persona Jurídica debe verificar:

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

La RA vinculada al PSC CODE100 S.A. verificará la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.7. CRITERIOS PARA INTEROPERABILIDAD

Podrán ser reconocidos los Certificados Digitales Extranjeros de conformidad a la normativa vigente. Para el efecto, el estado paraguayo deberá suscribir Acuerdos Internacionales con sus pares extranjeros, salvo que, por protocolo adicional a un tratado vigente, los países suscriptores del mismo hayan acordado el reconocimiento recíproco de los certificados digitales emitidos en los respectivos países.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES

No se permite la re emisión de claves.

3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RE EMISIÓN DE CLAVES DESPUÉS DE UNA REVOCACIÓN

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

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

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

- Mediante el código de revocación que es enviado al suscriptor en el correo consignado en el momento de la emisión del certificado.
- Presencialmente a través de los procesos de autenticación, de identidad (sección 3.2.3)
- Cualquier otro medio establecido por CODE100 S.A. y aprobado por el MIC que permita una identificación veraz y segura.

La revocación podrá ser iniciada por el Suscriptor, por el PSC CODE100 S.A. o su RA vinculada.

Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del PSC desde: http://www.code100.com.py/firma-digital/revocacion.html

Este sitio se encuentra disponible las 24 horas los 7 días de la semana, durante todo el año, lo que permite servicios de revocación en horarios no habituales de jornada laboral, como así también fines de semana y feriados. La solicitud de revocación se procesa automáticamente de acuerdo a lo establecido en el punto 4.9.5, tiempo dentro del cual el PSC CODE100 S.A. debe procesar la Solicitud de revocación.

En el caso de pérdida del PIN de revocación se deberá solicitar en el portal del Suscriptor el reenvío del mismo. Éste se enviará a la dirección informada por el Suscriptor, en forma automática.

EL PSC CODE100 S.A. o su RA vinculada podrán iniciar de oficio la revocación de certificados, según lo indicado en el "4.9.1.Circunstancias para la revocación" y se deja asentado en los registros informáticos del PSC CODE100 S.A. la revocación efectuada.

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

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

CODE100 S.A describe los requisitos y procedimientos operacionales conforme lo estipulado en la CP. Esos requisitos y procedimientos comprenden como mínimo:

a) La comprobación de los atributos de identificación que constan en el certificado conforme al ítem 3.

b) Una solicitud de certificado firmada por el titular del certificado o por el responsable del uso del certificado, en caso de la persona jurídica, conforme al FORMULARIO DE SOLICITUD DE CERTIFICADO correspondiente.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Las personas que pueden presentar una solicitud de certificado, que en el marco de la PKI Paraguay, son:

- Para el caso de certificado de persona física, toda persona, mayor de edad, sin distinción, con un documento de identidad válido, que será el sujeto a cuyo nombre se emita el certificado.
- Para el caso de certificado de persona jurídica, el representante legal o el responsable del uso del certificado con poder suficiente.
- Para el caso de certificado de equipo o aplicación, el representante legal o el responsable del uso del certificado con poder suficiente si el solicitante es una persona jurídica, o toda persona, mayor de edad, sin distinción, con un documento de identidad válido si el solicitante es una persona física.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Es atribución del PSC CODE100 S.A. dentro de la PKI Paraguay determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la Política de Certificación aplicable en cada caso. El PSC CODE100 S.A. podrá autorizar o denegar la solicitud de certificación. La denegatoria como excepción y en circunstancias debidamente fundadas.

Las solicitudes de los certificados, una vez completadas, serán enviadas al PSC CODE100 S.A.

CODE100 S.A. tiene la responsabilidad de:

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

Todo solicitante que desee un certificado deberá:

- Completar el formulario de solicitud del certificado con toda la información que CODE100 S.A. requiera para la emisión del mismo. Cabe destacar que no toda la información solicitada aparecerá en el certificado, asegurándose su conservación integra, de manera confidencial, por la Autoridad de Certificación.

- Entregar la solicitud de firma del certificado (CSR) a la RA, que incluye la clave pública, en el caso de que el par de claves lo haya generado el solicitante, y el certificado se genere directamente a partir de la solicitud. En la correspondiente CP se establecerá el procedimiento de entrega.

La existencia del formulario de solicitud y en general el procedimiento de solicitud de certificados queda definido en la Política de Certificación correspondiente a cada tipo de certificado.

4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

La RA vinculada al PSC CODE100 S.A. debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el punto 3.2

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

El PSC CODE100 S.A. o la RA vinculada a ella deben rechazar la solicitud de certificado en los casos que no se dé cumplimiento a la normativa vigente y a lo establecido en esta CPS.

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

El tiempo de procesamiento del CSR (lapso de tiempo entre la solicitud emitida a la CA y la emisión del certificado del suscriptor) cualquiera sea el caso, será en el menor tiempo posible.

El plazo será determinado en la CP.

4.3 EMISIÓN DEL CERTIFICADO

El certificado se considera válido desde el momento de su emisión.

4.3.1 ACCIONES DEL PSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

La emisión del certificado depende del correcto llenado del formulario de solicitud, de la firma del acuerdo de suscriptores y de la recepción de otros documentos requeridos de acuerdo con las especificaciones para cada tipo de certificado. Después del proceso de validación de la información proporcionada por el solicitante, se emite el certificado.

En caso que sean requeridos procedimientos específicos para cada CP implementadas por el PSC CODE100 S. A., los mismos serán descriptos, en el ítem correspondiente.

4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

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

Cada CP podrá establecer otro mecanismo de notificación mediante el que se informará al solicitante de la emisión de su certificado.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

El titular del certificado o la persona responsable verifica la información contenida en el certificado y la acepta si la información es completa, correcta y verdadera. De lo contrario, el titular del certificado no puede usar el certificado y debe solicitar inmediatamente su revocación. Al aceptar el certificado, el titular del certificado:

a) Acepta las responsabilidades, obligaciones y deberes en esta CPS y la CP correspondiente;

b) Asegura que, a su conocimiento, ninguna persona no autorizada ha tenido acceso a la clave privada asociada con el certificado;

c) Establece que toda la información contenida en el certificado, proporcionada en la solicitud, es verdadera y se reproduce en el certificado de manera correcta y completa.

La aceptación del certificado y su contenido será declarada por el titular del certificado expresamente con la firma del acuerdo de suscriptores. En caso de los certificados emitidos para personas jurídicas, equipo o aplicaciones, la declaración expresa será de la persona física responsable de ese certificado.

En caso que sea requeridos procedimientos específicos para las CP implementadas por el PSC CODE100 S. A., los mismos serán descriptos en esas CP, en el ítem correspondiente.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC

CODE100 S.A. publicará información de los certificados que emite a través de un mecanismo de consulta que estará disponible en el sitio:

http://www.code100.com.py/firma-digital/portal-suscriptor.html.

Además, CODE100 S.A. publica en su repositorio público su certificado digital y el de la CA raíz.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES

No se definen entidades externas que necesiten o requieran ser notificados acerca de los certificados emitidos por el PSC CODE100 S. A.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

El titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la CP correspondiente, de acuerdo con lo establecido en los campos **'Key Usage'** y **'Extended Key Usage'** del certificado y de la normativa vigente. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la CPS y CP, y sólo para lo que éstas establezcan.

Tras la expiración o revocación del certificado, el titular deberá dejar de usar la clave privada.

En caso que sean requeridos procedimientos específicos para las CP implementada por el PSC CODE100 S. A., los mismos serán descriptos en esas CP, en el ítem correspondiente.

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA

La parte que confía podrán depositar su confianza en los certificados emitidos por el PSC CODE100 S. A. en concordancia con lo establecido en el campo 'Key Usage, 'Extended Key Usage' del certificado, y la normativa vigente.

4.6 RENOVACIÓN DEL CERTIFICADO

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

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADOS

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 EL PSC DEL CERTIFICADO RENOVADO

No aplica.

4.6.7 NOTIFICACIÓN POR EL PSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

No aplica.

4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

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

4.7.1 CIRCUNSTANCIAS PARA 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 EL PSC DE LOS CERTIFICADOS RE-EMITIDOS

No aplica.

4.7.7 NOTIFICACIÓN POR EL PSC 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

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

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 EL PSC DE LOS CERTIFICADOS MODIFICADOS

No aplica.

4.8.7 NOTIFICACIÓN POR LA CA DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

No aplica.

4.9 REVOCACION Y SUSPENSION

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Un certificado deberá obligatoriamente ser revocado en las siguientes circunstancias:

a) 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) Que afectan la seguridad de la clave o del certificado:

- Compromiso de la clave privada o de la infraestructura o sistemas del PSC que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente;
- Infracción, por el PSC CODE100 S. A. de los requisitos previstos en los procedimientos de gestión de los certificados, establecidos en su propia CP y CPS;
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del titular del certificado;
- Acceso o utilización no autorizada, por un tercero, de la clave privada del titular;
- El uso irregular por el titular, 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 de la clave privada del titular del certificado;

d) Circunstancias que afectan al suscriptor

- Infracción del titular del certificado en sus obligaciones, responsabilidad y garantías, establecidas en la CP y CPS del PSC que emitió el certificado;
- La incapacidad de hecho sobrevenida o la muerte del titular del certificado;
- La extinción de la persona jurídica titular del certificado;
- Solicitud de revocación del certificado por su titular de acuerdo con lo establecido en la CP y en la CPS.

e) Otras causales especificadas en la normativa y reglamentación vigente.

4.9.2 QUIEN PUEDE SOLICITAR REVOCACIÓN

La revocación de un certificado sólo podrá realizarse:

- Por petición del titular del certificado;
- Por solicitud del responsable del certificado en el caso de un certificado de persona jurídica o un certificado de maquina o aplicación;
- Por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado, funcionario o servidor;
- Por CODE100 S.A. en su condición de PSC emitente;
- Por una RA vinculada a el PSC CODE100 S.A.
- Por determinación de la CA Raíz del Paraguay;
- Por una autoridad judicial competente.

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Quienes están autorizados a solicitar la revocación, conforme al ítem 4.9.2, pueden, fácilmente y en cualquier tiempo, solicitar la revocación de sus respectivos certificados.

Como directrices generales se establece que:

a) El Solicitante de revocación de un certificado debe ser identificado;
b) Las solicitudes de revocación, así como las acciones resultantes de ellas serán registrada y almacenadas;
c) Se documentarán las razones de la revocación de un certificado;
d) La revocación de un certificado terminará con la generación y publicación de una CRL que contenga los datos del certificado revocado y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PSC CODE100 S.A.

El plazo máximo admitido para la conclusión del proceso de revocación del certificado después de la recepción de la respectiva solicitud, para todos los certificados descriptos en esta CPS, será de 12 (doce) horas.

En el caso que sean requeridos procedimientos específicos para las CP implementadas por el PSC CODE100 S. A., los mismos serán descriptos en esas CP, en el ítem correspondiente.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

No se estipula periodo de gracia para revocación de certificados.

4.9.5 TIEMPO DENTRO DEL CUAL EL PSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

El proceso de solicitud de revocación debe ser inmediato cuando están configuradas las circunstancias definidas en el ítem 4.9.1. El plazo máximo admitido para la conclusión del proceso de revocación del certificado después del recibimiento de la respectiva solicitud, para todos los certificados descriptos en esta CPS es de 12 (doce) horas.

En caso que sean requeridos plazos específicos para la CP de CODE100 S. A. implementadas, los mismos serán descriptos en esas CP, en el ítem correspondiente, que no podrán superar las 12 horas.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

Las partes que confían deben evaluar el estado del certificado y el estado de todos los certificados de la CA en la cadena a la que pertenece el certificado, antes de confiar en él.

Para ello, las partes que confían pueden verificar el estado del certificado mediante el servicio de: OCSP o CRL más reciente, provista por el PSC.

4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

La CRL se actualizará y publicará inmediatamente cuando surja una revocación o:

- Con una frecuencia de emisión máxima permitida de 12 (doce) horas para la CRL referente a los usuarios finales.
- Con una frecuencia de emisión máxima permitida de 3 meses para la CRL referente al PSC.

CODE100 S.A. publicará periódicamente una única lista conteniendo todos los certificados revocados por ella, en forma acumulativa, en formato del CRL X.509 v2, sin superar las doce (12) horas entre publicaciones. Además cuando surja la revocación del certificado de un Suscriptor, la PSC CODE100 S.A. generará y publicará una nueva CRL.

En caso que sean utilizadas frecuencias de emisión específicos de CRL para las CP de CODE1OO S. A. implementadas, serán descriptos en esas CP, en el ítem correspondiente.

4.9.8 LATENCIA MÁXIMA PARA CRL

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

En caso de que sean requeridas la latencia máxima para la CRL, específicas para las CP de CODE100 implementadas, serán descriptos en esas CP, en el ítem correspondiente.

4.9.9 REQUISITOS DE VERIFICACIÓN DEL CRL

CODE100 S.A. mantendrá disponible un repositorio con información del estado de los certificados emitidos, el cual puede ser accedido vía web. Adicionalmente, CODE100 S.A. implementa el servicio de validación en línea OCSP.

Todo certificado deberá tener su validez verificada, en la respectiva CRL, antes de utilizarlo.

La autenticidad de la CRL deberá también ser confirmada, por medio de la verificación de la firma del PSC emitente en el periodo de validez de la CRL.

4.9.10 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 el PSC CODE100 S.A. que estará disponible en su sitio principal de internet. Adicionalmente CODE100 S.A. implementa el servicio de validación en línea por medio del protocolo OCSP (On-line Certificate Status Protocol).

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.

4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

Los terceros que confían deberán verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección 4.9.10.

En caso de ser requeridos procedimientos específicos para las CP de CODE1OO S. A. implementadas, los mismos serán descriptos en esas CP, en el ítem correspondiente.

4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE |REVOCACIÓN DISPONIBLES

Este Ítem no aplica.

4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

El compromiso de la clave privada del PSC CODE100 S.A. será notificado, en la medida posible, a todos los participantes de la PKI Paraguay, en especial a:

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

El PSC CODE100 S.A., deberá notificar en un plazo de 24 horas como máximo a la DGFD&CE respecto a circunstancias que produzcan el compromiso de sus claves o su imposibilidad de uso.

Además el PSC CODE100 S.A. publicará el compromiso de su clave en su sitio principal de Internet y procederá a la inmediata gestión de la revocación de su certificado y el de sus suscriptores.

CODE100 S.A. publicará el certificado revocado en el repositorio.

El compromiso de la clave privada del suscriptor de un certificado emitido por el PSC CODE100 S. A. deberá ser comunicada el hecho inmediatamente al mismo identificándose según lo establecido en el punto 3.4.

4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN

No aplica.

4.9.15 QUIEN PUEDE SOLICITAR LA SUSPENSIÓN

No aplica.

4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

No aplica.

4.9.17 LÍMITES DEL PERÍODO DE SUSPENSIÓN

No aplica.

4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

El estado de los certificados emitidos por el PSC CODE100 S. A. está disponible a través de su CRL publicado en la siguiente dirección: https://ca1.code100.com.py/firma-digital/crl/ca-code100.crl.

El PSC CODE100 S.A. publicará información de los certificados que emite a través de un mecanismo de consulta que estará disponible en el sitio:

http://www.code100.com.py/firma-digital/portal-suscriptor.html.

Además implementa el servicio de validación en línea por medio del protocolo OCSP.

4.10.2 DISPONIBILIDAD DEL SERVICIO

Los sistemas de distribución de CRLs y de consulta en línea del estado de los certificados están disponibles de forma ininterrumpida todos los días del año, tanto para las Partes que confían como para los Suscriptores u otras partes que lo requieran.

El PSC CODE100 garantiza la disponibilidad del servicio de publicación en el repositorio público de la CRL, del Sistema de Consulta de Certificados Emitidos,

y el servicio de consulta en línea por medio del protocolo OCSP con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3 CARACTERÍSTICAS OPCIONALES

Sin estipulaciones.

4.11 FIN DE LA SUSCRIPCIÓN

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

- Revocación del certificado, por cualquiera de las causas establecidas en la presente política, antes del vencimiento (fecha de expiración).
- Expiración del certificado.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

El PSC CODE100 S. A. no custodia claves de los suscriptores de ningún certificado.

Para los efectos del "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio", la clave privada del PSC CODE100 S.A. está custodiada y respaldada bajo estrictas normas de seguridad, y almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3, que garantizan la no divulgación de las claves.

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

En los ítems siguientes, son descriptos los controles de seguridad implementados por el PSC CODE100 SA y por sus RA vinculadas, para ejecutar de modo seguro sus funciones de generación de claves, identificación, certificación, auditoria y respaldo de los registros.

5.1 CONTROLES FÍSICOS

En las secciones siguientes, la CPS describe los controles físicos referentes a las instalaciones que albergan los sistemas del PSC CODE100 SA y de sus RA vinculadas.

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La localización de las instalaciones donde se albergan los sistemas de certificación del PSC CODE100 SA, no es públicamente identificada. No existe identificación pública externa de las instalaciones e internamente, no es admitido ambientes compartidos que permiten la visibilidad de las operaciones de emisión y revocación de los certificados. Esas operaciones son segregadas en compartimientos cerrados y físicamente protegidos.

En las instalaciones del PSC CODE100 SA, se implementaron, entre otros, los siguientes controles:

a) Instalaciones para equipamientos de apoyo, tales como: máquinas de aire acondicionado, grupos de generadores, UPS, baterías, paneles de distribución de energía y de telefonía;

b) Instalaciones para sistemas de telecomunicaciones;

c) Los sistemas de puesta a tierra y protección contra rayos; y

d) Iluminación de emergencia;

Las instalaciones donde se emiten los certificados del PSC CODE100 SA, se protegen con su propio y único perímetro físico, y las barreras físicas (paredes y barrotes) son sólidas, extendiéndose desde el piso real al techo real.

5.1.2 ACCESO FÍSICO

El PSC CODE100 S.A. implementa un sistema de control de acceso físico que garantiza la seguridad de sus instalaciones, conforme al ítem 9 "control de accesos" de la norma ISO 27002:2013 y los siguientes puntos:

5.1.2.1 NIVELES DE ACCESO FÍSICO

Para acceder al primer nivel de acceso físico se requiere que todo individuo sea identificado y registrado por el personal autorizado. En este perímetro no se realizará ninguna operación ni proceso administrativo del PSC CODE100 S.A..

Excepto en los casos previstos por la ley, la posesión de armas no será admitida en las instalaciones del PSC CODE100 S.A., desde el

nivel 1. A partir de ese nivel, las personas extrañas a la operativa del PSC CODE100 S.A. deberán transitar debidamente identificadas y acompañadas, los equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles, será controlado su ingreso y sólo pueden ser utilizados mediante la autorización formal y supervisada.

Para acceder al segundo nivel de acceso físico se requiere de un factor de autenticación y tarjeta de identificación visible. En este perímetro, se desarrollan procesos administrativos del PSC CODE100 S.A.. Este ambiente es interno al primer nivel.

Para acceder al tercer nivel de acceso físico se requieren de 2 (dos) factores de autenticación electrónica y tarjeta de identificación visible. Se sitúa dentro del segundo nivel y es el primer nivel en albergar material y actividades sensibles de la operativa del PSC CODE100 S.A.. Cualquier actividad relativa al ciclo de vida de los certificados digitales estará localizada a partir de este nivel. Personas que no están involucradas con esas actividades no deberán tener permiso para acceder a este nivel. Personas que no poseen permiso de acceso no podrán permanecer en este nivel si no estuviesen acompañadas por alguien que tenga permiso de acceso.

En este nivel son controladas tanto las entradas como las salidas de cada persona autorizada.

Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PSC CODE100 S.A., no son aceptadas desde el nivel 3.

Para acceder al cuarto nivel de acceso físico se requieren de 2 (dos) factores de autenticación (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, se exige, en cada acceso a su ambiente, la identificación de 2 (dos) personas autorizadas.

En este nivel se realizan actividades especialmente sensibles a la operación del PSC CODE100 S.A., tales como la emisión y revocación de los certificados y la emisión de la CRL. Todos los sistemas y equipamientos necesarios a estas actividades están localizados a partir de este nivel. En este nivel, la permanencia de esas personas es exigida mientras el ambiente estuviera ocupado.

En el cuarto nivel, todas las paredes, piso y techo están revestidos con material resistente. Las paredes, piso y techo

están construidas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de comunicación no permiten la penetración física en las áreas de cuarto nivel. Adicionalmente, tienen una protección contra las interferencias electromagnéticas externas.

Este ambiente fue construido según las normas internacionales aplicables.

En el PSC CODE100 S.A., existen varios ambientes del cuarto nivel para albergar y segregar, cuando fuera el caso:

a) Equipamientos de producción on-line y cofre de almacenamiento;

b) Equipamientos de producción of-line y cofre de almacenamiento; y

c) Equipamientos de redes e infraestructura (firewall, ruteadores, switches y servidores).

El quinto nivel de acceso físico es interno al ambiente del nivel 4 y constituye un cofre, donde están almacenados: materiales criptográficos, tales como, claves, datos de activación, sus copias y equipamientos criptográficos

Para garantizar la seguridad del material almacenado, el cofre obedece las siguientes especificaciones mínimas:

a) Estar hecho de acero o con material de resistencia equivalente; y

b) Poseer cerraduras antirrobo.

El sexto nivel de acceso físico, es interno al ambiente del nivel 4 y constituye un gabinete reforzado. Los datos de activación de la clave privada del PSC CODE100 S.A. están almacenados en ese ambiente.

Para garantizar la seguridad del material almacenado, el gabinete obedece las siguientes especificaciones mínimas:

a) Estar hecho de acero o con material de resistencia equivalente; y

b) Poseer cerraduras antirrobo.

Sistemas físicos de detección: la transición entre los diferentes perímetros de acceso, así como la sala de operaciones del nivel 4, son monitoreadas por cámaras de video ligadas a un sistema de grabación 24x7. El posicionamiento y la capacidad de estas cámaras no permiten recuperar las contraseñas digitadas en los controles de acceso.

Las cintas de vídeo resultantes de grabación 24x7 son almacenadas, como mínimo, 1(un) año. Ellas son testeadas (verificación de estrechos aleatorios en el inicio, medio y final de la cinta) por lo menos cada 3(tres) meses, con la elección, como mínimo, de 1(una) cinta referente a cada semana. Esas cintas están almacenadas en el ambiente del nivel 3.

Todas las puertas de transición entre los ambientes de niveles 3 y 4 son monitoreadas por un sistema de notificación de alarmas. Donde hubiere, a partir del nivel 2, vidrios separando niveles de acceso, es implementado un mecanismo de alarma de quiebra de vidrios, que estará funcionando ininterrumpidamente.

En todos los ambientes del cuarto nivel, una alarma de detección de movimientos permanece activo hasta que se satisfaga el criterio de acceso al ambiente.

Los sistemas de notificación de alarmas utilizan 2(dos) medios de notificación: sonoro y visual.

El sistema de monitoreo de las cámaras de video, así como el sistema de notificación de alarma, están permanentemente monitoreados por el personal autorizado en el ambiente de nivel 3 están localizados en el nivel 3. Las instalaciones del sistema de monitoreo, a su vez, son monitoreados por cámaras de vídeo cuyo posicionamiento permite el seguimiento de las acciones del personal autorizado.

Sistema de control de acceso: el sistema de control de acceso está en el ambiente de nivel 4.

Mecanismos de emergencia: mecanismos específicos son implementados por el PSC CODE100 S.A. para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia. Esos mecanismos permiten el desbloqueo de las puertas por medio de accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada por medio de estos mecanismos accionan inmediatamente las alarmas de apertura de puertas.

Todos los procedimientos de los mecanismos de emergencia están documentados. Los mecanismos y procedimientos de emergencia son verificados semestralmente, por medio de simulación de situaciones de emergencia.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

Las áreas donde se ubican los equipos de la infraestructura tecnológica del PSC CODE100 S.A. cuentan con suministros de electricidad y aire acondicionados adecuados a los requisitos de los equipos en ellas instalados. La infraestructura se encuentra protegida contra caídas de tensión o cualquier otra anomalía en el suministro eléctrico. El PSC CODE100 S.A. dispone de:

- Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés Uninterruptible Power Supply)
- Grupo electrógeno con potencia suficiente para soportar la carga del Data Center, incluido los equipos informáticos y equipos de refrigeración.
- Doble Acometida eléctrica para los equipos.
- Sistema puesta a tierra implantado.
- Tuberías, conductos, canaletas, paneles y cajas (de paso, distribución y terminación) diseñadas y construidas de forma a facilitar la inspección y detección de intentos de manipulación.

Todos los cables están catalogados e identificados. Los mismos son inspeccionados al menos cada (6) meses, en busca de evidencia de violación y anomalías.

Son mantenidos actualizados los registros sobre la topología de red de cables, de acuerdo a los requisitos de confidencialidad establecidos en el ítem 13 "seguridad en las telecomunicaciones" de la norma ISO 27002/2013. Cualquier modificación en esa red deberá ser previamente documentada.

No son admitidas instalaciones provisorias, cableados expuestas o directamente conectadas a tomas sin utilización de conectores adecuados.

El Sistema de climatización cumple con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente y dispone de filtros de polvos. En los ambientes del nivel 4, el sistema de climatización es independiente y tolerantes a fallas.

La temperatura de los ambientes atendido por los sistemas de climatización es permanentemente monitoreada por el sistema de notificación de alarmas.

Los sistemas de aire acondicionados de los ambientes de nivel 4 son internos, con cambio de aire realizados apenas por la abertura de la puerta.

La capacidad de redundancia de toda la estructura de energía y aire acondicionado es garantizada, por medio de:

a) Generadores de un tamaño compatible

b) Generadores de reserva;

c) Sistemas de UPS redundantes; y

d) Sistemas redundantes de aire acondicionado.

La estructura interna al ambienta de nivel 4, provee protección física contra exposición a agua, filtraciones e inundaciones provenientes de cualquier fuente externa.

5.1.4 EXPOSICIONES AL AGUA

Las instalaciones del PSC CODE100 S.A. están protegidas para evitar exposiciones al agua, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

El sistema de prevención contra incendios, internos a los ambientes posibilitan alarmas preventivas antes que el humo sea visible, activados solamente con la presencia de partículas que caracterizan el sobrecalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

En las instalaciones del PSC CODE100 S.A. no está permitido fumar o portar objetos que produzcan fuego o chispa.

El nivel 4 posee un sistema para detección precoz de humo y un sistema de extinción de incendio por gas.

En caso de incendio de las instalaciones del PSC CODE100 S.A., o el aumento la temperatura interna del ambiente del nivel 4, no deberá exceder 50 grados Celsius, y el ambiente deberá soportar esta condición, como mínimo, 1 (una) hora.

5.1.6 ALMACENAMIENTO DE MEDIOS

La información relacionada a la infraestructura del PSC CODE100 S.A. se almacena de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida. Los cofres de seguridad son de acero o material de resistencia equivalente, debe ofrecer resistencia:

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

- Posee tranca con llave manual, es suficientemente pesado, de forma a dificultar su retiro.

5.1.7 ELIMINACIÓN DE RESIDUOS

Los documentos y materiales sensibles son triturados antes de su eliminación.

Todos los dispositivos electrónicos que ya no son utilizables y que se han utilizado previamente para el almacenamiento de información sensible son destruidos físicamente.

5.1.8 RESPALDO FUERA DE SITIO

El PSC CODE100 S.A. cuenta con una instalación alterna con niveles de protección física y ambiental similar al sitio principal y con una separación física adecuada. En caso de siniestro que torne inoperante la instalación principal del PSC CODE100 S.A., las instalaciones de respaldo no se vean afectadas y tomen totalmente las operaciones del PSC CODE100 S.A. en condiciones idénticas en, un máximo, de 48(cuarenta y ocho) horas.

5.1.9 INSTALACIONES TÉCNICAS DE LA RA

Las instalaciones técnicas de la RA vinculadas al PSC CODE100 S.A. cumplen con los requisitos establecidos en el documento **CARACTERISTICAS MINIMAS DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO DEL PARAGUAY.**

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

Cuando un empleado se desvincula del PSC CODE100 S.A., sus permisos de accesos son revocados inmediatamente. Cuando hay un cambio en la posición o función que el empleado ocupa dentro del PSC, sus permisos de accesos son revisados. Existe una lista de revocación, con todos los recursos, antes disponibilidades, que el empleado deberá devolver al PSC CODE100 S.A. en el momento de su desvinculación.

Los roles contemplan, las siguientes responsabilidades que a continuación serán descriptos:

a) **Responsables de seguridad:** debe llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobadas por el PSC CODE100 S.A., controlar la formalización de

los convenios entre el personal y el PSC CODE100 S.A., comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, debe cumplir y hacer cumplir las políticas de seguridad del PSC CODE100 S.A. 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 del PSC CODE100 S.A..

b) **Responsables de coordinación de área:** es el responsable de autorizar tecnológicamente la emisión de un certificado o la revocación del mismo. Bajo su control y supervisión, se encuentra el personal adscripto a la misma. Es su responsabilidad:
   - Recibir y dar curso a las denuncias que podrían afectar a su personal, proponiendo las medidas disciplinarias correspondientes
   - Efectuar un control permanente de la adecuación de los recursos materiales y humanos que cuenta el área a su cargo, con el fin de atender las necesidades de servicio que tiene encomendadas

c) **Responsables de sistemas:** los responsables de este rol no 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 del PSC CODE 100 S.A. y asumen la gestión de los servicios de ruteo 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 del PSC y de la eliminación del hardware criptográfico del PSC de la producción. Serán responsables del mantenimiento o reparación de equipos criptográficos PSC (incluida la instalación de nuevo hardware, firmware, software), y la eliminación de desmontaje y permanente por el uso.

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

e) **Responsables de auditoría interna:** 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) **Responsables 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.

Responsable Técnico: Es quien opera el sistema de gestión de certificados y el HSM, uso de las claves del 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) **Responsables de desarrollo de sistemas del PSC:** 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.

h) **Responsable de Recursos Humanos:** es el responsable de analizar antecedentes laborales, facilitar condiciones para la evaluación de la idoneidad técnica, implementar controles de Seguridad personal, entregar los materiales correspondientes al rol a desempeñar, confeccionar legajos de antecedentes laborales, calificaciones personales.

i) **Responsable Legal:** es el responsable de mantener actualizados los requisitos legales exigidos, elaborar y administrar los contratos, participar en la capacitación del personal en materia legal, asistir a los conflictos derivados de la operatoria del PSC.

j) **Responsable de Contingencia:** se encarga de proponer actividades de capacitación en estos temas, aprobar las pruebas de contingencia, planificar y realizar simulacros de recuperación frente a desastres.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

El PSC CODE100 S.A. dispone de requisito de control multi-usuarios para la generación y la utilización de la clave privada del PSC responsable, de la forma definida en el ítem 6.2.2.

Todas las tareas ejecutadas en el ambiente donde está localizado el equipamiento de certificación del PSC CODE100 S.A. requiere, como mínimo, de 2(dos) empleados con rol de confianza. Las demás tareas del PSC CODE100 S.A. son ejecutadas por un único empleado.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Todo empleado que asume un rol de confianza en el PSC CODE100 S.A. es identificado y su perfil es verificado antes de que:

a) Sean incluido en una lista de acceso a las instalaciones del PSC CODE100 S.A.;

b) Sean incluido en una lista para acceso físico al sistema de certificación del PSC CODE100 S.A.;

c) Reciban un certificado electrónico para ejecutar sus actividades operacionales en el PSC CODE100 S.A.; y

d) Reciban una cuenta de usuario del sistema de certificación del PSC CODE100 S.A.

Los certificados, cuentas y contraseñas utilizados para la identificación y autenticación de los empleados deberán:

a) Ser directamente asignados a un único empleado;

b) No ser compartidos; y

c) Restringirse a las acciones asociadas con el perfil para el que fueron creados.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

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

- Un oficial criptográfico no puede ser responsable de auditoría interna.
- Un administrador de sistemas no puede ser ni coordinador de seguridad ni responsable de auditoría.
- Un coordinador de seguridad no puede ser administrador de sistemas ni oficial de registro, ni oficial de activación, ni responsable de auditoría interna.
- Un responsable de auditoría interna no podrá cumplir otra función o rol.

Además otras tareas que son segregadas son:

- La validación de información en aplicaciones de certificado y de solicitudes información del suscriptor.
- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación.
- La emisión o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La emisión o destrucción de los certificados del PSC CODE100 S.A.
- La puesta en operación del PSC CODE100 S.A en producción.

5.3 CONTROLES DE PERSONAL

5.3.1 REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Todo el personal del PSC CODE100 S.A. responsable y de la RA vinculada e involucrada en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados es seleccionado y admitido, conforme a lo establecido en el ítem 7 "seguridad ligada a los recursos humanos" de la norma ISO 27002/2013 y además deben:

a) Haber demostrado capacidad para ejecutar sus deberes;

b) Haber suscripto un acuerdo de confidencialidad y disponibilidad;

c) No poseer otros deberes que puedan interferir o causar conflicto con los del PSC CODE100 S.A.;

d) No tener antecedentes de negligencia o incumplimiento de labores; y

e) No tener antecedentes penales.

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PSC CODE100 S.A. y de la RA vinculada involucrada en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados son sometido a:

- Confirmación de empleos anteriores.
- Verificación de referencias profesionales.
- Título académico obtenido.
- Verificación de antecedentes judiciales y policiales.

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Todo personal del PSC CODE100 S.A. y de la RA involucrada en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, recibe la formación necesaria para asegurar la correcta realización de sus funciones tales como:

- Principios y mecanismos de seguridad del PSC CODE100 S.A. y de la RA.
- Sistema de certificación en uso del PSC CODE100 S.A..
- Procedimientos de recuperación de desastres y continuidad del negocio;
- Reconocimiento de firmas y validación de documentos presentados en los ítem 3.2.2., 3.2.3. y 3.2.4.;
- Normativa vigente que rige la materia; y
- Otros asuntos relacionados con las actividades bajo su responsabilidad.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PSC CODE100 S.A. y de la RA vinculada, involucrada en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados es mantenido y actualizado sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PSC CODE100 S.A. o de la RA.

El PSC CODE100 S.A. y de la RA vinculada provee programas de entrenamiento y actualización a su personal para asegurar que el personal mantenga el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

EL PSC CODE100 S.A. y las RA vinculadas efectúan una rotación de sus roles de confianza como mínimo una vez cada 3 años.

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

En la eventualidad de una acción no autorizada, real o sospechosa, realizada por una persona encargada del proceso operacional del PSC CODE100 S.A. o de su RA vinculada, CODE100 S.A. procederá de inmediato, la suspensión de acceso de esa persona al sistema de certificación e iniciará un procedimiento administrativo para determinar los hechos y, si es necesario, tomar las medidas legales pertinentes.

El proceso administrativo referido en el párrafo anterior contendrá, como mínimo, los siguientes puntos.

- Relato de lo ocurrido con el modo de operación;
- Identificación de los involucrados;
- Eventuales perjuicios causados;
- Las sanciones aplicadas, si fuere el caso; y

Conclusiones.

Concluido el proceso administrativo, el PSC CODE100 comunicará sus conclusiones a la CA Raíz.

Las sanciones que podrían aplicarse como resultado de un procedimiento administrativo son:

- Advertencia;
- Suspensión por un plazo determinado; o
- Impedimento definitivo de ejercer funciones en el ámbito de la PKI Paraguay.

5.3.7 REQUISITOS DE CONTRATACIÓN A TERCEROS

Todo el personal del PSC CODE100 S.A. su RA, involucrada en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, es contratado conforme a lo establecido los ítems 7 "seguridad ligada a los recursos humanos" y 15 "relaciones con suministradores" norma ISO 27002/2013 y bajo las siguientes condiciones mínimas:

- Que exista un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.
- Que el PSC CODE100 S.A. o su RA no posea personal disponible para llenar los roles de confianza.

- Que el personal a contratar cumpla con los mismos requisitos del ítem 5.3.1.
- Que una vez finalizado el servicio contratado se revoquen los derechos de acceso.

5.3.8 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

El PSC CODE100 S.A. pone a disposición de todo el personal del PSC CODE100 S.A. y para todo el personal de su RA al menos:

- Su CPS;
- Las CP que implementa;
- La política de seguridad que implementa el PSC;
- Documentación operacional relativa a sus actividades; y
- Contratos, normas y políticas relevantes para sus actividades.

Toda documentación entregada o disponibilizada al personal están clasificadas y actualizadas.

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

5.4.1 TIPOS DE EVENTOS REGISTRADOS

El PSC CODE100 S.A. registra en archivos de auditoria todos los eventos relacionados a la seguridad del sistema de certificación. Entre otros los siguientes eventos están incluidos en los archivos de auditoria:

a) Iniciación y terminación del sistema de certificación;
b) Los intentos de crear, eliminar, establecer contraseña o cambiar los privilegios del sistema de los operadores del PSC;
c) Los cambios en la configuración del PSC o en sus llaves;
d) Los cambios en las políticas de creación de certificados;
e) Los intentos de accesos (login) y de salida del sistema (logoff);
f) Los intentos no autorizados de acceso a los archivos del sistema;
g) La generación de claves propias del PSC CODE100 S.A. o de claves de sus usuarios finales;
h) La emisión y revocación de certificados;
i) La generación de la CRL;

j) Los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;

k) Las operaciones fallidas de escritura o lectura en el repositorio de los certificados y de la CRL, en su caso; y

l) Las operaciones de escritura en ese repositorio, en su caso.

EL PSC CODE100 S.A. registra, electrónicamente o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

a) Registros de accesos físicos;

b) El mantenimiento y los cambios en la configuración de sus sistemas;

c) Los cambios de personal y los cambios de su rol de confianza;

d) Los informes de discrepancia y de compromiso; y

e) El registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados, o de la información personal de los usuarios.

Se prevé que todos los registros de auditoria, electrónicos o manuales, contengan la fecha y hora del evento y la identidad del agente que lo causo.

Para facilitar los procesos de auditoria, toda la documentación relacionada a los servicios del PSC CODE100 S.A. es almacenada, electrónicamente o manualmente, en un local único, conforme a lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2013.

La RA vinculada al PSC CODE100 S.A., registra electrónicamente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los certificados. Los siguientes eventos están incluidos en los archivos de auditoria:

a) Los agentes de registros que realizan las operaciones;

b) Fecha y hora de las operaciones;

c) La asociación entre los agentes que realizan la validación, aprobación y el certificado generado;

d) La firma digital del ejecutante.

El PSC CODE100 S.A. a la que está vinculada la RA, establece en un documento que esté disponible en las auditorias de cumplimiento, el local de archivos de las copias de los documentos utilizados para la identificación del suscriptor, presentados en el momento de la solicitud y revocación de certificados. El formulario de solicitud y el acuerdo de suscriptores.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Se establece un periodo no superior a 1 (un) mes, con que los recursos de auditoria serán analizados por el personal operacional. Todos los eventos significativos son explicados en un informe de auditoría de registros. Tal análisis involucra una inspección breve de todos los registros, con la verificación de que no fueron alterados, seguida de una investigación más detallada de cualquier alerta o irregularidades en esos registros. Todas las medidas adoptadas como resultado de este análisis son documentadas.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

El PSC CODE100 S.A., mantiene localmente sus registros de auditoria por los menos 2 (dos) meses y, consecuentemente, es almacenado de la manera descripta en el ítem 5.6.2.

Además de las revisiones oficiales, los registros de auditoría son revisados en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas del PSC CODE100 S.A.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

El PSC CODE100 S.A. protege sus registros de auditoria contra lectura no autorizada, modificación y eliminación. Además establece mecanismos obligatorios de protección de información manual de auditoria contra la lectura no autorizada, modificación y eliminación.

Los mecanismos de protección descriptos en este ítem obedecen a lo dispuesto en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2013.

5.4.5 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA

El PSC CODE100 S.A. generara copias de seguridad de los registros de auditorías y su frecuencia, que no debe ser superior a 1 (un) mes.

5.4.6 SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)

Los archivos de registro son almacenados en los sistemas internos, mediante una combinación de procesos automáticos y manuales ejecutados por las aplicaciones del PSC CODE100 S.A.

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Cuando un evento es registrado por el conjunto de sistemas de auditoria del PSC CODE100 S.A., no se requiere notificar al causante de dicho evento, a excepción de que el evento sea de índole accidental y resulta probable que pueda volver a ocurrir.

5.4.8 EVALUACIÓN DE VULNERABILIDADES

Los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoria del PSC CODE100 S.A., serán analizadas detalladamente y, dependiendo de su gravedad, registradas por separado. Acciones correctivas que surjan serán implementadas por el PSC CODE100 S.A. y registradas con fines de auditoria.

5.5 ARCHIVOS DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Los tipos de registros archivados, comprenden entre otros:

- **Durante el inicio de operaciones del PSC CODE100 S.A.:**
  a) La habilitación en caso del PSC CODE100 S.A. o una RA;
  b) La CP y la CPS;
  c) Cualquier acuerdo contractual para establecer los límites del PSC CODE100 S.A. o RA vinculada; y
  d) La configuración del sistema que requiere el PSC CODE100 S.A..
- **Durante la operativa del PSC CODE100 S.A.:**
  a) Modificaciones o actualizaciones de cualquiera de los ítems anteriores;
  b) Solicitudes de certificados;
  c) Solicitudes de revocación de certificados;
  d) Documentación para autenticar la identidad del titular del certificado y del responsable de su uso en el caso de un certificado de persona jurídica o un certificado de equipamiento o aplicaciones;
  e) Documentación de recepción de dispositivos de almacenamiento de claves;
  f) Todos los certificados emitidos;
  g) Todas las CRL emitidas y publicadas;

h) Notificaciones de compromiso de clave privada;

i) Informaciones de auditorías previstas en el ítem 5.4.1;

j) Todos los trabajos comunicados o relacionados a políticas, otras PSC y 5.5.2

5.5.2 PERIODOS DE RETENCIÓN PARA ARCHIVOS

Se establecen periodos de retención para cada registro archivado, teniendo en cuenta que:

a) La CRL y los certificados emitidos de firma digital deben ser conservados permanentemente para fines de consulta histórica;

b) Las copias de los documentos para identificación del suscriptor, presentados en el momento de la solicitud y de la revocación de certificados, el formulario de solicitud y el acuerdo de suscriptores, como mínimo, por 10 (diez) años, a contar desde la fecha de expiración o revocación del certificado; y

c) Las demás informaciones, inclusive los archivos de auditoria, deberán ser almacenadas, como mínimo, 10 años.

5.5.3 PROTECCIÓN DE ARCHIVOS

Todos los registros archivados son clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, conforme a lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2013.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Una segunda copia de todo el material archivado es almacenada en un local externo al PSC CODE100 S.A., recibiendo el mínimo tipo de protección utilizada para el archivo principal.

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

El PSC CODE100 S.A. debe verificar la integridad de esas copias de seguridad, como mínimo, cada 6(seis) meses.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

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.

El responsable de la RA vinculada realiza pruebas de restauración de la información archivada al menos 1 (una) vez al año.

5.6 CAMBIO DE CLAVE

El PSC CODE100 S.A. debe cambiar su clave de acuerdo con el tiempo de uso y tiempo operacional de los certificados emitidos dentro de la PKI Paraguay, este cambio técnicamente implica la emisión de un nuevo certificado.

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

Nivel de Jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de Suscriptores (Módulo Hardware)	2	2	El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez
Certificado de Suscriptores (Módulo	1	1	El certificado emitido al usuario final es otorgado por un tiempo máximo de un año, al finalizar ese período pierde su validez

Software)			
Certificado del PSC CODE100 S.A.	8	10	El Certificado emitido al PSC tendrá: Un tiempo operacional de 10 años, que resulta de la suma del tiempo de uso de su certificado (8 años) más el tiempo de validez máximo del certificado de su suscriptor (2 años). Solamente durante el tiempo de uso de su certificado, el PSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional solo podrá firmar el CRL de usuarios o suscriptores.

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

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

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

El PSC CODE100 S.A. tiene la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1 PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Los requisitos relacionados a los procedimientos de notificación y de recuperación de desastres, previstos en el plan de continuidad del negocio del PSC CODE100 S.A., se establecen conforme a lo establecido en el ítem 16

"gestión de incidentes en la seguridad de la información" de la norma ISO 27002/2013, para garantizar la continuidad de sus servicios críticos.

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

En el caso de compromiso de la clave privada, el PSC CODE100 S.A. 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 del PSC ya no son válidos.

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

CODE 100 S.A. cuenta y mantiene un "Plan de Contingencia, Recuperación frente a Desastres y Continuidad del Negocio" de manera que en el evento de una interrupción del negocio, las funciones críticas puedan ser recuperadas. Para ello la CA cuenta con una instalación de recuperación de desastres en un sitio alterno localizado en una instalación separada geográficamente del sitio principal. Este sitio alterno está 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 del PSC CODE100 S.A., el equipo técnico informado 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.

El tiempo objetivo para recuperar la funcionalidad del servicio de Producción crítico es no mayor que 24 horas.

Los procedimientos de recuperación utilizados por la CA de CODE100 S.A. está conforme a lo establecido en el ítem 17 "aspectos de seguridad de la información en la gestión de la continuidad del negocio" de la norma ISO 27002:2013

5.7.5 ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO

El PSC CODE100 S.A. establece en su Plan de continuidad del Negocio de las RA vinculadas para la recuperación, total o parcial de sus operaciones, las siguientes actividades:

a) Identificación de eventos que pueden causar interrupciones en los proceso del negocio, por ejemplo falla de equipamientos, inundación e incendios;

b) Identificación y concordancias de todas las responsabilidades y procedimientos de emergencia con los roles afectados;

c) Implementación de procedimientos de emergencia que permitan la recuperación y restauración en los plazos necesarios. La evaluación de la recuperación de la documentación almacenada en instalaciones técnicas afectadas por el desastre;

d) Documentación de los procesos y procedimientos acordados;

e) Entrenamiento adecuado del personal en los procedimientos y procesos de emergencia definidos, incluido el gerenciamiento de crisis;

f) Prueba y actualización de los planes.

5.8 EXTINCIÓN DE UN PSC

En caso que el PSC CODE100, deje de operar deberá cumplir, como mínimo, con lo siguiente:

a) Publicar en su sitio principal de internet la fecha de suspensión de los servicios con al menos 60 días de anticipación;

b) Publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese de las operaciones;

c) Notificar a sus suscriptores por lo menos 30 días antes de la suspensión efectiva o cese de sus operaciones

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

En caso que el PSC CODE100 S.A., deje de operar, no podrá bajo ningún sentido emitir ningún certificado pero deberá continuar dando soporte a las operaciones de revocación de certificados y publicación de CRL. Recién una vez vencidos o revocados todos los certificados emitidos, y cuya revocación esté publicada, cesa automáticamente la responsabilidad del PSC.

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

El MIC custodiará toda la información referida al cese de operación del PSC, además publicará el cese de actividades o finalización del servicio del PSC CODE100 S.A. en su sitio principal de internet.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

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 oSigning Operations - Protection Profile CMCSO-PP).

Toda CA debe elaborar un documento en el que especifique 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 generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública generada bajo el control PSC CODE100 S.A. 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 control del usuario final es entregada al PSC CODE100 S.A. 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 CODE100 S.A., 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 es obtenido del repositorio que está a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de comprobación.

6.1.5 TAMAÑO DE LA CLAVE

El tamaño de las claves criptográficas de la CA de CODE100 S.A. es de 4096 bits. El tamaño de las claves para cada tipo de certificado emitido por CODE100 S.A. viene definido por la Política de Certificación que le sea de aplicación.

6.1.6 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

Se prevé que los parámetros de generación de claves asimétricas del PSC CODE100 S.A. adoptara el patrón definido en el documento **NORMAS Y ALGORITMOS CRIPTOGRAFICOS DE LA PKI PARAGUAY.**

Los parámetros de verificación de calidad, son verificados de acuerdo con las normas establecidas por el patrón definido en el documento **NORMAS DE ALGORITMOS CRIPTOGRAFICOS DE LA PKI PARAGUAY.**

6.1.7 PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X509 V3)

La clave privada del PSC CODE100 S.A. es utilizada únicamente para la firma de los certificados emitidos por ella y de sus CRL.

6.1.8 GENERACIÓN DE CLAVE POR HARDWARE O SOFTWARE

El proceso de generación del par de claves del PSC CODE100 S.A., es realizado en un módulo criptográfico de hardware que cumple, con el estándar FIPS 140-2 nivel 3.

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 CODE100 S.A. para la creación de las claves cumplen 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.

Los módulos criptográficos de generación de claves asimétricas del PSC CODE100 S.A. adoptan los patrones definidos en el documento NORMAS Y ALGORITMOS CRIPTOGRAFICOS DE LA PKI PARAGUAY.

Cada CP implementada debe especificar los requisitos adicionales aplicables.

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

Cuando sea el caso, debe ser definida la forma de control múltiple, de tipo "N" personas de un grupo "M", requerido para la utilización de las claves privadas.

El control multi-persona establecido en la CP, garantiza que nadie tenga el control de forma individual y completa de las actuaciones críticas. Como mínimo serán requeridos 3(tres) de "M" titulares de activación de clave, formalmente designada por el PSC.

6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA

La custodia de la clave privada del certificado la realizan los propios titulares de la misma, teniendo en cuenta que no se permitirá en el ámbito de la PKI Paraguay, almacenar clave privada del titular del certificado de firma digital (tipo F) emitido por el PSC..

6.2.4 RESPALDO/COPIA DE LA CLAVE PRIVADA

Cualquier entidad titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

EL PSC CODE100 S.A mantiene una copia de seguridad de su propia clave privada.

El PSC CODE100 S.A no mantiene copia de seguridad de la clave privada del titular de certificado de firma digital por ella emitida.

El PSC CODE100 S.A podrá por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado o cliente, mantener una copia de seguridad de la clave privada correspondiente al certificado de cifrado por ella emitida.

En cualquier caso, la copia de seguridad debe ser almacenada cifrada por un algoritmo simétrico definido en el documento NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY, y protegida con un nivel de seguridad no inferior a aquel definido para la calve original.

6.2.5 ARCHIVADO DE LA CLAVE PRIVADA

Las claves son archivadas en un nivel de seguridad no inferior a aquella definida para la clave original. No son archivadas las claves privadas de la firma digital.

Defínase archivado como el almacenamiento de la clave privada para su uso futuro, después del periodo de validez del certificado correspondiente.

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

El PSC CODE100 S.A. mantiene almacenada su clave privada original y su copia de seguridad en módulos criptográficos de hardware que cumple, con el estándar FIPS140-2 nivel 3.

El PSC no mantiene almacenada la clave privada del titular de certificado de firma digital por ella emitida.

Por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado o cliente, el PSC podrá mantener almacenada una copia de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada CP debe definir los requisitos específicos aplicables.

En cualquier caso, la clave privada deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

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 multi-persona. El medio de almacenamiento de clave privada se restablece a los valores predeterminados para que no quede información confidencial.

La destrucción de la clave privada debe constar en los registros de auditoría.

6.2.11 CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

El módulo criptográfico del PSC CODE100 S.A., cumple mínimamente el estándar FIPS 140-2, nivel 3.

Cuando sea el caso, la CP implementada debe describir la clasificación del módulo criptográfico utilizado por las entidades titulares de los certificados.

6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas del PSC CODE100 S.A. y de los titulares de los certificados de firma digital, así como las CRL emitidas, son almacenadas por CODE100 S.A., después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

6.3.2 PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES

La clave privada del PSC CODE100 S.A. y de los titulares de certificados de firma digital, deberá ser utilizada únicamente durante el periodo de validez estipulado en el ítem 5.6. La clave pública podrá ser utilizada durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

6.4 DATOS DE ACTIVACIÓN

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la clave privada del PSC CODE100 S.A., son únicos y aleatorios.

La CP debe garantizar que los datos de activación de la clave privada del titular del certificado, serán únicos y aleatorios.

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 del PSC CODE100 S.A., 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.

Los datos de activación de clave privada del PSC CODE100 S.A. están protegidos contra el uso no autorizado a través de encriptación y mecanismos de control de acceso físico.

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

La generación del par de claves del PSC CODE100 S.A. se realiza offline para impedir el acceso remoto no autorizado.

Cada computador del PSC CODE100 S.A., relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificado, deberá implementar, entre otras, las siguientes características:

a) Control de acceso a los servicios y perfiles del PSC;

b) Clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PSC;

c) Uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;

d) Generación y almacenamiento de registros de auditoria dl PSC;

e) Mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y

f) Mecanismos para copias de seguridad (backup).

Estas características deberán ser implementadas por el sistema operativo o por medio de combinación de este con el sistema de certificación y con mecanismos de seguridad física.

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento deberán haber borrado la información confidencial que contenga y controlar su número de serie y las fechas de envío y recepción. Al regresar a las instalaciones de CODE100 S.A., el equipo que fue sometido a mantenimiento debe ser inspeccionado. Cualquier equipo que ya no se utilice de forma permanente, deberán ser destruidas de él, de manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad de CODE100 S.A.. Todos estos eventos deberán ser registrados con fines de auditoría.

Cualquier equipo incorporado en CODE100 S.A. será preparado y configurado según lo previsto en la política de seguridad implementada u otro documento relevante con el fin de mostrar el nivel de seguridad requerido para su propósito.

Los requisitos específicos aplicables deben ser descriptos en cada CP implementada.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

La seguridad informática del PSC CODE100 S.A. sigue las recomendaciones de los Criterios de evaluación del sistema de confianza (TCSEC).

6.5.3 CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

La RA está instalada en un ambiente, que cumple con las siguientes condiciones:

a) Equipos de prevención de incendios.

b) Armario o gabinete con llave, de uso exclusivo de la RA, para mantener protegidos los documentos de la RA.

c) Una única puerta de entrada, con cerradura de seguridad, con apertura preferentemente a través del uso de una tarjeta de identificación soportada en un medio electrónico.

d) Paredes que prevengan el acceso no autorizado, construidas con material que no sea desmontable y que cubra toda la altura del ambiente, asegurando que no existan pasos por debajo de pisos flotantes y por arriba de cielorrasos suspendidos.

e) Iluminación de emergencia.

f) En caso de que el ambiente posea ventanas u otras aberturas hacia el exterior, éstas deben estar selladas o enrejadas para impedir el acceso externo.

g) Guardia de seguridad.

Como mínimo se incluyen los requisitos especificados en el documento **CARACTERÍSTICAS MINÍMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY.**

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 que cumplan con la FIPS 140-2 nivel 2.
- Los procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación después de la ceremonia de generación de claves.

6.6.4 CONTROLES EN LA GENERACIÓN DE CRL

Antes de su publicación, todas las CRL generadas por el PSC CODE100 S.A., es comprobada la consistencia de su contenido, comparándolo con el contenido esperado en relación al número el CRL, la fecha / hora de emisión otras informaciones relevantes.

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1 DIRECTRICES GENERALES

Se describen a continuación los controles relativos a la seguridad de red del PSC CODE100 S.A., incluidos firewalls y recursos similares.

En los servidores del sistema de certificación del PSC, solo los servicios estrictamente necesarios para el funcionamiento de la aplicación deben estar habilitados.

Todos los servidores y elementos de la infraestructura y protección de redes, tales como ruteadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red en que se hospeda el sistema de certificación del PSC, están localizados y operan en un ambiente de nivel, como mínimo, 4 (cuatro).

Las últimas versiones de los sistemas operativos y servidores de aplicaciones, así como las eventuales correcciones (parches), disponibilizadas por los respectivos fabricantes deberán ser implementadas inmediatamente después del testeo en el ambiente de homologación.

El acceso lógico a los elementos de la infraestructura y protección de la red deberán restringirse por medio de un sistema de autenticación y autorización de acceso. Los Ruteadores conectados a redes externas deberán implementar filtros de paquetes de datos, que solo permitan conexiones a los servicios y servidores previamente definidos como objeto de acceso externo.

6.7.2 FIREWALL

Mecanismos de Firewall se implementan en equipos de uso específico, configurado exclusivamente para esa función. Un firewall promueve el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona desmilitarizada" (DMZ) – en relación a los equipos con acceso exclusivamente interno al PSC.

El Software del firewall, entre otras características, implementa registros de auditoria.

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

El Sistema de detección de intruso tiene la capacidad de ser configurado para reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar traps SNMP, ejecutar programas definidos por el administrador de la red, enviar emails a los administradores, enviar mensaje de alertas al firewall o la terminal de gerenciamiento, promover la desconexión automática de las conexiones sospechosas, o la reconfiguración del firewall.

El sistema de detección de intrusiones es capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de actuar su base de conocimiento.

El sistema de detección de intruso promueve un registro de eventos en logs, recuperables en archivos de tipo texto, e implementa una gestión de la configuración.

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Los intentos de acceso no autorizados en los routers, Firewalls u IDS son registrados en archivos para posterior análisis, que podrá ser automatizada. La frecuencia de los exámenes de los archivos de registro es, como mínimo, diario y todas las acciones tomadas como resultado de dicho examen son documentadas.

6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

El modulo criptográfico de la CA adopta el estándar definido en el documento **NORMAS DE ALGORITOMO CRIPTOGRAFICOS DE LA PKI PARAGUAY.**

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1 PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PSC CODE100 S.A. están conforme al formato definido por la norma ITU X.509 o ISO/IEC 9594-8.

- ITU-T X.509 V.3 Information technology Open systems interconnection The Directory: Public-key and attribute certificate frameworks
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- ETSI TS 101 862 V.1.3.3 Qualified Certificates Profile

- RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile
- ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".
- RFC – 3279 ' Internet X.509 Public Key Infrastructure Algorithm Identifier"

A continuación se detalla el contenido de las extensiones más importantes del Certificado del PSC CODE100 S.A.

CAMPO	COMPONENTE PROPUESTO	CRITICA
1. Version	V3	
2. Signature Algorithm	Sha256RSA	
3. Issuer	CN = AUTORIDAD CERTIFICADORA RAIZ DEL PARAGUAY O = Ministerio de Industria y Comercio C = PY	
4. Validez	10 AÑOS	
5. Subject	CN = CA-CODE100 S.A. C = PY O = CODE100 S.A. SERIALNUMBER = RUC 80080610-7	
6. Subject Public Key Info	Algoritmo: RSA Encryption Longitud:4096 bits	
7. Certificate Policies • Policy Identifier • URL CPS • Notice Referente	SE UTILIZARÁ Directivas del Certificado http://www.acraiz.gov.py/cps/politicas.pdf Certificados emitidos dentro del marco de la PKI Paraguay bajo la jerarquía de su ACRaíz	
8. CRLDistributionPoints	http://www.acraiz.gov.py/arl/ac_raiz_py.crl	NO
9. Auth. Information Acces • CAIssuers • OCSP	Se utilizará http://www.acraiz.gov.py/crt/ac_raiz_py_sha256.crt http://ca1.code100.com.py/ocsp	NO
10. BasicConstraints	Tipo de asunto=Entidad de certificación (CA)	SI

	Restricción de longitud de ruta=0	
11. KeyUsage	Firma de Certificado (Certificate Signing) Firma de CRL (CRL Signing).	SI
12. Subject Key Identifier	SHA-1 hash de la clave pública	NO
13. Authority Key Identifier • KeyIdentifier • AuthorityCertIssuer • AuthorityCerSerialNumber	Se utilizará SHA-1 hash de la clave pública del emisor No utilizado No utilizado	NO

7.1.1 NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PSC CODE100 S.A. soportan y utilizan la versión 3 (tres) del estándar ITU X.509, de acuerdo con el perfil establecido en la RFC 5280

7.1.2 EXTENSIONES DEL CERTIFICADO

Las extensiones utilizadas de forma genérica en el certificado del PSC CODE100 S.A. son:

a) "***Authority Key Identifier***", **no crítica:** el campo key Identifier debe contener el hash SHA- 1 de la clave pública del PSC que emite el certificado;

b) "***Subject Key Identifier***", **no crítica**: debe contener el hash SHA- 1 de la clave pública del PSC titular do certificado;

c) "***Key Usage***", **crítica**: solamente los bits keyCertSign e cRLSign deben estar activados;

d) "***Certificate Policies***", **no crítica**: el campo debe contener el OID de la CP que el PSC titular del certificado implementa y/o la dirección la dirección URL donde se encuentra disponible.

e) "***Basic Constraints***", **crítica**: debe contener el campo SubjectType CA=True y el campo PathLenConstraint debe tener valor cero; y

f) "**CRL Distribution Points", no crítica**: debe contener la URL donde está disponible el certificado de CRL.

7.1.3 IDENTIFICADORES DE OBJETO DE ALGORITMOS

Los certificados del PSC CODE100 S.A. son firmados utilizando el algoritmo definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

7.1.4 FORMAS DEL NOMBRE

Los nombres del PSC CODE100 S.A., referente a la extensión subject del certificado, adopta el "Distinguished Name" (DN) del estandar ITU X509 y es la que se describe como ejemplo en la siguiente tabla:

CAMPO	VALOR DE EJEMPLO
CN	CA-CODE100 S.A.
C	PY
O	CODE100 S.A.
SERIALNUMBER	RUC 80080610-7

7.1.5 RESTRICCIONES DEL NOMBRE

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

Los nombres se escriben en mayúsculas y sin tildes, únicamente se acepta el carácter "Ñ" como un caso especial para los nombres de personas físicas y jurídicas

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

Son restringidos conforme a las restricciones generales establecidas por la PKI Paraguay en el documento **DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DEL LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)**

7.1.6 IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

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

7.1.7 USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)

No aplica.

7.1.8 SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)

En los certificados del PSC CODE100 S.A., la extensión "Certificate Policies", contiene la URL de la CPS.

7.1.9 SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES)

No aplica.

7.2 PERFIL DE LA CRL

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

Campo	Valor o restricciones
Versión (Version)	Ver sección "7.2.1 Numero (s) de versión"
Algoritmo de firma (SignatureAlgorithm)	Algoritmo usado para la firma del CRL, puede ser como mínimo SHA256WithRSAEncryption
Emisor (Issuer)	Entidad que emite y firma la CRL.

Fecha efectiva (Effective Date)	Fecha de emisión de la CRL.
Siguiente actualización (NextUpdate)	Fecha para la cual es emitida la siguiente CRL. La frecuencia de emisión del CRL está acorde con lo requerido en la sección "4.9.7 Frecuencia de emisión de la CRL"
Certificados revocados (CertificateRevoked)	Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación.
Extensiones	
Número CRL (CRL Number)	Orden secuencial de emisión de CRL
Identificador de clave de Autoridad (Authority Key Identifier)	Identificador de la clave pública de la CA.
Punto de distribución del CRL (DistribuitionPoints)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado.

7.2.1 NÚMERO (S) DE VERSIÓN

Las CRL generadas se implementan con la versión 2 del CRL definido en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

La PKI Paraguay define como obligatorias las siguientes extensiones de CRL:

a) "Authority Key Identifier", no critica: debe contener el hash SHA-1 de clave pública de la PSC que firma la CRL; y

b) "CRL number" no critica: debe contener el número secuencial para cada CRL emitida.

7.2.2.1 NÚMERO CRL (CRL NUMBER)

Orden secuencial de emisión de CRL. Calificada como crítica.

7.2.2.2 IDENTIFICADOR DE CLAVE DE AUTORIDAD

El método para la generación del identificador está basado en la clave pública del PSC CODE100 S.A. de acuerdo a lo descrito por el RFC 5280 "Internet X.509 Public Key Infraestructura Certificate and CRL Profile". La extensión no es crítica.

7.3 PERFIL DE OCSP

El servicio de validación de certificados en línea OCSP (Online Certificate Status Protocol) es una forma para obtener información reciente sobre el estado de un certificado.

El servicio OCSP que implementa el PSC CODE100 S.A. cumple con lo estipulado en el RFC-2560 "X.509Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.1 NÚMERO (S) DE VERSIÓN

El PSC CODE100 S.A. cumple con la versión 1 del RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.2 EXTENSIONES DE OCSP

Sin estipulaciones.

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

El Art. 42 de la Ley Nro. 4017/2010 establece que los PSC, deben ser auditados periódicamente, de acuerdo con el sistema de auditoría que diseñe y apruebe el MIC.

Por Resolución Ministerial se establece el sistema de auditoría al cual será sometido el PSC.

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

El MIC o terceros designados por él, será responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la normativa vigente.

Cada PSC, debe implementar un programa de auditorías internas conforme a lo estipulado en el sistema de auditoria que diseñe el MIC y lo establecido en el ítem 18 "cumplimiento" de la norma ISO 27002/2013 para la verificación de su sistema de gestión.

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

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Se llevará a cabo una auditoría externa al PSC CODE100 S. A. de forma regular al menos una vez al año y los costos serán asumidos CODE100 S. A. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta CPS, las CP y la normativa vigente.

El PSC CODE100 S.A. realizará una auditoría interna al menos una vez al año

8.2 IDENTIDAD/CALIDADES DEL EVALUADOR

Todo equipo o persona designada para realizar una auditoría al PSC de CODE100 S.A. deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en tecnología de PKI, criptografía, tecnología de la información y seguridad.
- Independencia a nivel organizativo del PSC CODE100 S. A.

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Para el caso de las Auditorías externas, los Auditores deben ser independientes e imparciales, quienes ejecutarán las evaluaciones acordes a los procedimientos establecidos.

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

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Los aspectos cubiertos por la Auditoría son:

- Controles de seguridad física y estándares técnicos de seguridad;
- Confidencialidad y calidad de los sistemas de control;
- Integridad y disponibilidad de los datos;
- Cumplimiento de los estándares tecnológicos;

- Seguridad del personal;
- Cumplimiento de la política y declaración de prácticas de certificación;
- Procesos de certificación de clave pública;
- Política de seguridad y privacidad;
- Controles administrativos del PSC,
- Administración de los servicios del PSC; y
- Revisión de contratos.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

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

En caso de detectarse una irregularidad en la Auditoría externa realizada al PSC CODE100 S.A., EL MIC en su calidad de CA Raíz podrá tomar entre otras las siguientes acciones dependiendo de la gravedad de la misma:

- Indicar las irregularidades, pero permitir al PSC CODE100 S.A. que continúe sus operaciones hasta la próxima Auditoría programada;
- Permitir al PSC CODE100 S.A. que continúe sus operaciones con un máximo de treinta días corridos, tiempo durante el cual deberá subsanar la irregularidad detectada, caso contrario se procederá a la Suspensión; o
- Suspender la operación del PSC CODE100 S.A. o sus RA vinculadas.

En caso que el MIC ordene la suspensión de actividades del PSC CODE100 S.A, solo se podrá realizar servicios de soporte técnico y atención a los suscriptores ya existentes, en ningún caso podrá seguir brindando servicios de certificación.

8.6 COMUNICACIÓN DE RESULTADOS

El equipo auditor comunicará los resultados de la auditoría a la Autoridad de Aplicación, al Coordinador de Seguridad del PSC CODE100 S.A. así como a gerencia de PSC CODE100 S.A. y de la Autoridad en la que se detecten incidencias.

El PSC CODE100 S.A. publicará en su sitio principal de internet los informes relevantes de las auditorías realizadas.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

El PSC CODE100 S.A. se encuentra obligado a cumplir con las tasas y aranceles impuestos por la normativa vigente.

EL PSC CODE100 S.A. deberá comunicar al interesado en adquirir un certificado digital, todos los costos que deberá asumir para la obtención del certificado.

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Los certificados digitales emitidos bajo la presente CPS son expedidos a favor de personas físicas y de personas jurídicas a título oneroso, aplicándose aranceles diferenciales asociados conforme a la clase de certificado:

Los aranceles serán publicados en el sitio web CODE100 S.A. al que se accede mediante:

http://www.code100.com.py/firma-digital/aranceles.html

El solicitante/suscriptor del certificado deberá pagar el arancel de su certificado. Con el comprobante para el pago emitido a ese efecto, podrá abonar en la RA o en los medios de pago que se indican en la siguiente dirección

http://www.code100.com.py/firma-digital/aranceles.html

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

El PSC CODE100 S. A. no se encuentra habilitado para el cobro de tarifas de acceso a certificados.

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

El PSC CODE100 S.A. no se encuentra habilitada para el cobro de tarifas de acceso a estado o revocación de los certificados.

9.1.4 TARIFAS POR OTROS SERVICIOS

EL PSC CODE100 S.A., no se encuentra habilitada para el cobro de tarifas para acceder a información de las Políticas de Certificación y la Declaración de Prácticas de Certificación.

9.1.5 POLÍTICAS DE REEMBOLSO

La Política de Reembolsos del PSC CODE100 S.A. comprende los Certificados Digitales que emite bajo sus Políticas de Certificación.

Ante las siguientes circunstancias:

- El solicitante presenta un reclamo sobre un certificado digital emitido por el PSC CODE 100 S.A. dentro de los 15 días posteriores a su fecha de emisión,
- Y dicho reclamo se fundamenta en la existencia de una falla en el certificado u error en la emisión del mismo por parte del PSC CODE100 S.A.
- El PSC CODE100 S.A. podrá, otorgar un reembolso de la totalidad del importe abonado por el solicitante para los certificados con fallos u errores, o emitir nuevamente el certificado objetado sin costo alguno.
- Pasados 15 días de la fecha de emisión del certificado, se entenderá total aceptación del certificado emitido y del servicio brindado por el PSC CODE100 S.A., y no se realizarán reembolsos ni devoluciones de ningún tipo.

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

El PSC CODE100 S.A. cuenta con un medio de garantía suficiente para cubrir las actividades inherentes a su gestión de conformidad con lo establecido en la normativa vigente.

9.2.2 OTROS ACTIVOS

El PSC CODE100 S.A. posee suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes, asimismo es razonablemente capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

No estipulado.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

La clave privada de firma digital del PSC CODE100 S.A. es generada y mantenida por el propio PSC que será responsable de mantener su confidencialidad. La divulgación o utilización indebida de la clave privada de firma digital por el PSC, será de su entera responsabilidad.

Los titulares de certificados emitidos para personas físicas o sus responsables para el uso de los certificados emitidos para personas jurídicas, equipos o aplicaciones, tendrán las atribuciones de generación, y confidencialidad de sus respectivas claves privadas.

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

La protección abarca a la siguiente información, en la medida en que no sea de conocimiento público:

- Toda la información remitida por el solicitante o suscriptor a la RA, excepto los datos que figuran en el certificado.
- Cualquier información almacenada en servidores o bases de datos destinadas a firma digital.
- Cualquier información impresa o transmitida en forma verbal referida a procedimientos, manual de procedimientos, etc., salvo aquellos que en forma expresa fueran declarados como no confidenciales.
- Cualquier información referida a planes de contingencia, controles o procedimientos de seguridad, registros de auditoría creados y/o mantenidos por CODE100 S.A.

La presente lista es de carácter ilustrativo, resultando confidencial toda información del proceso de firma digital que expresamente no señale lo contrario. La regla general es que toda información que no sea considerada como pública revestirá el carácter de confidencial.

Durante el ciclo de vida del certificado, tanto el PSC CODE100 S.A. como sus RA vinculada no podrán divulgar los datos de los suscriptores sin su consentimiento. Asimismo, el PSC CODE100 S.A. se compromete a hacer público exclusivamente los datos del suscriptor que resulten imprescindibles para el reconocimiento de su firma digital.

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

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

- La contenida en la presente Declaración de Prácticas de Certificación.
- La incluida en las Políticas de certificación que le sean de aplicación.
- Los certificados emitidos por el PSC CODE100 S.A.
- La lista de los certificados revocados.
- Las versiones públicas de la PSS.
- La conclusión de los informes de auditoría.

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

CODE100 S.A. implementa políticas de privacidad de información, de acuerdo con la normativa vigente. No se puede divulgar o vender información de los suscriptores o información de identificación de éstos.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

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

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

El tratamiento de la información que no es considerada como privada, está sujeta a lo que dispone la normativa vigente al efecto. Únicamente se considera pública la información contenida en el certificado. Algunos de ellos se citan en la sección 9.3.2.

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

El personal que desempeñe labores en el PSC CODE100 y sus RA vinculadas, que tenga acceso a los datos considerados privados se encuentra constreñida a proteger la información y deben estar obligados contractualmente a ello.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

La información privada no puede ser usada sin el consentimiento de las partes. Consentida, el PSC CODE100 S.A. no requiere notificar a los suscriptores para usar información privada.

9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

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

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

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

9.5 DERECHO DE PROPIEDAD INTELECTUAL

El PSC CODE100 S.A. es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS así como de las correspondientes CP. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de CODE100 S.A. sin la autorización expresa por su parte.

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC

El PSC CODE100 S.A. es responsable del cumplimiento de sus obligaciones, según se establecen en esta CPS, incluso aunque parte de su actividad sea realizada mediante contratación externa.

El PSC CODE100 S.A. tiene las siguientes obligaciones:

- Operar de acuerdo con su CPS y CP que implementa;
- Generar y gestionar sus pares de claves criptográficas;
- Asegurar la protección de sus claves privadas;
- Notificar a la CA raíz, emisor de su certificado, cuando se presenta el compromiso de su clave privada y solicitar la revocación inmediata del correspondiente certificado;

- Notificar a sus usuarios cuando hay una sospecha de compromiso de su clave privada o una nueva emisión de su par de claves o la terminación de prestación de su servicio;
- Distribuir su propio certificado;
- Emitir, expedir y distribuir los certificados de las RA a ellas vinculadas, y de los usuarios finales;
- Informar la emisión del certificado al respectivo solicitante;
- Revocar los certificados por el emitidos;
- Emitir, gerenciar y publicar sus CRL y disponibilizar la consulta online de la situación de los certificados emitidos (OCSP - On-line Certificate Status Protocol);
- Publicar, en su sitio principal internet, su CPS, y las CP aprobadas que implementa;
- Publicar, en su sitio principal de Internet, las informaciones definidas en el ítem 2.2. De este documento;

  Publicar, en su sitio principal internet, las informaciones sobre la desvinculación de una RA, así como la extinción de la instalación técnica.
- Utilizar protocolo de comunicación segura para proporcionar servicios a los solicitantes y usuarios de certificados digitales a través de la web;
- Identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por la Autoridad de Aplicación.
- Adoptar las medidas de seguridad y de control previstas en la CPS, CP y políticas de seguridad (PS) que se implementa, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por la Autoridad de Aplicación.
- Mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por la Autoridad de Aplicación y la normativa vigente;
- Mantener y garantizar la integridad, confidencialidad y seguridad de la información por ella tratada;
- Mantener y anualmente realizar prueba de su Plan de Continuidad de Negocios (PCN);
- Mantener el contrato de seguro de responsabilidad civil resultante de las actividades de certificación digital y de registro, con una cobertura suficiente y compatible con el riesgo de estas actividades.
- Informar a terceras partes y los titulares de certificados sobre las garantías, cobertura, condiciones y limitaciones establecidas a la póliza

de seguro de responsabilidad civil contraída en los términos indicado en el inciso t) de este ítem;

- Informar a la CA raíz, mensualmente, la cantidad de certificados digitales emitidos y revocados;
- No emitir el certificado con una fecha de caducidad que se extienda más allá de la fecha de vencimiento de su propio certificado.

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

Las RA vinculadas Al PSC CODE100 S.A. deben cumplir las siguientes obligaciones:

- Recibir las solicitudes de emisión y revocación de los certificados;
- Confirmar la identidad del solicitante y validar la solicitud;
- Comunicar la solicitud de emisión o revocación del certificado al psc
- Responsable utilizando un protocolo de comunicación segura, conforme al
- Patrón definido en el documento. **CARACTERÍSTICAS MÍNIMAS DE**
- **SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY**
- Informar a los respectivos titulares la emisión o revocación de sus certificados;
- Proporcionar los certificados emitidos por el PSC a sus respectivos solicitantes;
- Identificar y registrar todas las acciones ejecutadas, conforme a las normas,
- Prácticas y reglas establecidas por el MIC y la normativa vigente;
- Mantener el cumplimiento de sus procesos, procedimientos y actividades
- Con las normas, criterios, prácticas y reglas establecidas por el PSC
- Vinculado, el MIC y en especial con lo contenido en el documento
- Características mínimas de seguridad para las RA de la PKI
- Paraguay;
- Mantener y garantizar la seguridad de la información por ella tratada, de
- Acuerdo a lo establecido en las normas, criterio, prácticas y procedimientos
- Establecidos por el MIC;
- Mantener y anualmente realizar prueba de su plan de continuidad de negocios (PCN);
- Proceder al reconocimiento de las firmas y de la validez de los documentos presentados en la forma de los ítems 3.2.2, 3.2.3 y 3.2.4.
- Garantizar que todas las aprobaciones de la solicitud de certificados sean realizadas en las instalaciones técnicas autorizadas para funcionar como RA.

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

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

- Proporcionar, de manera completa y precisa, toda la información necesaria para su identificación;
- Garantizar la protección y confidencialidad de sus claves privadas, contraseñas y dispositivos criptográficos;
- Utilizar sus certificados y claves privadas de una manera apropiada, según lo dispuesto en la CP correspondiente;
- Conocer sus derechos y obligaciones, contemplados por la CPS y CP correspondiente y otros documentos aplicables la PKI PARAGUAY; y
- Informar al PSC emisora cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

En el caso de certificado emitido a las personas jurídicas, equipo o aplicación, estas obligaciones se aplican al responsable del uso certificado.

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

La parte que confía, es aquel que confía en el contenido, validez aplicabilidad del certificado digital. Constituyen derechos de la tercera parte:

- Negarse a utilizar el certificado para fines distintos de los previstos en la CP correspondiente.
- Comprobar, en cualquier momento, la validez del certificado. Un certificado emitido por un PSC integrante de la PKI Paraguay es considerado valido cuando:
  - No figura en la CRL del PSC emisor;
  - No estuviera expirado; y
  - Se pueda verificar usando el certificado válido del PSC emisor.

La falta de ejercicio de estos derechos no elimina la responsabilidad del PSC CODE100 S.A. y del titular del certificado.

9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO.

El repositorio público de la PSC CODE100 S. A. debe:

- Disponibilizar, inmediatamente después de su emisión, los certificados emitidos por la CA y su CRL.
- Estar disponible para consulta durante 24 (veinticuatro) horas al día, siete (7) días a la semana; y
- Aplicar los recursos necesarios para la seguridad de los datos almacenados en él.

9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

No aplica

9.7 EXENCIÓN DE GARANTÍA

El PSC CODE100 S.A. solo responderá en el caso de incumplimiento de las obligaciones contenidas en Ley Nº 4017/2010, Ley Nº 4610/2014, decreto N° 7369/2011, en la presente CPS y en las Políticas de Certificación específicas.

El PSC CODE100 S.A. sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

EL PSC CODE100 S.A. no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

El PSC CODE100 S.A. no asume ninguna responsabilidad en caso de cualquier tipo de pérdida o perjuicio:

- De los servicios que presta, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta CPS.
- Ocasionados por el mal uso de la información contenida en el certificado.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la PSC
- El PSC CODE100 S.A. no asumirá responsabilidad alguna en relación con el uso de los Certificados emitidos por su CA y el par de claves privada/pública asociado a sus titulares para cualquier actividad no especificada en la CPS o en las Políticas de Certificación correspondientes.

- El PSC CODE100 S.A como Prestador de Servicios de Certificación, no será responsable del contenido de los documentos electrónicos, ni mensajes de datos firmados con sus certificados ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado o comunicaciones.

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

A excepción de lo establecido por las disposiciones de la presente CPS, en la Ley Nº 4017/2010, Ley Nº 4610/2014, su decreto reglamentario Nº 7369/2011, el PSC CODE100 S.A. no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían.

9.9 INDEMNIZACIONES

El PSC CODE100 S. A. indemniza a los suscriptores por cualquier causa legalmente establecida, se debe demostrar ante las autoridades correspondientes los daños y perjuicios causados por sus actos y/u omisiones.

Además se establecen las causas de indemnización de los suscriptores al PSC:

- 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

Esta CPS 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 de CODE100 S. A. estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión, en ese caso, también se retirará del repositorio público del PSC CODE100 S.A.

9.10.3 EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

La finalización de la vigencia de la CPS del PSC CODE100 S.A, 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 CPS contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

9.11 NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

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

9.12 ENMIENDAS

9.12.1 PROCEDIMIENTOS PARA ENMIENDAS

Los cambios efectuados en la CP y CPS de los PSC CODE100 S.A. deben ser revisados y aprobados por la Dirección General de Firma Digital y Comercio Electrónico, antes de que éstos sean implementados. La documentación puede requerir una revisión.

9.12.2 PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Toda enmienda o modificación de la CPS y las CP implementadas por el PSC CODE100 S. A., se publicarán en su sitio principal de internet.

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 contendrá una cláusula de resolución de disputas.

El PSC CODE100 S.A. 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 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 de la República del Paraguay con renuncia a su propia jurisdicción si fuese otra.

Esta CPS no prevalece sobre las normas, criterios, prácticas y procedimientos establecidos por el MIC.

9.14 NORMATIVA APLICABLE

El PSC CODE100 S.A. estará sujeto a las leyes de la República del Paraguay, en particular a la normativa que rige la materia.

9.15 ADECUACIÓN A LA LEY APLICABLE

La responsabilidad del MIC en su calidad de Autoridad de Aplicación es la de velar por el cumplimiento de la legislación aplicable indicada en el apartado anterior.

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

Los Acuerdos de Suscriptores incluyen cláusulas de fuerza mayor para proteger al PSC CODE100 S.A.

9.17 OTRAS DISPOSICIONES

La CPS y las CP de CODE100 S.A., guardan concordancia con las disposiciones de la presente Declaración de Prácticas de la CA Raíz de la jerarquía de la PKI Paraguay.

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.

- Resolución N° 1401/2016 del MIC "Por la cual se autoriza en carácter experimental, por el término de doce meses, la emisión de certificados de firma digital en módulo software para persona física".
- CP y CPS de la CA raíz del Paraguay.
- Directivas Obligatorias Para La Formulación Y Elaboración De La Práctica De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Directivas Obligatorias Para La Formulación Y Elaboración De La Política De Certificación De Los Prestadores De Servicios De Certificación (PSC) V1.0
- Características Mínimas De Seguridad Para La Autoridades De Registro De La Infraestructura De Claves Públicas Del Paraguay V 1.0
- Normas De Algoritmos Criptográficos PKI-Paraguay V1.0