code100 S.A.
SERVICIOS DE CERTIFICACION DIGITAL

POLÍTICA DE CERTIFICACIÓN

VERSIÓN 1.4 – FECHA 28/04/2015

CLASE: PÚBLICO

Versiones y modificaciones de este documento

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	2014-04-04	GrupoFD	Directorio CODE100	Aprobación para presentación
1	1	2014-12-10	GrupoFD	Directorio CODE100	Aprobación para presentación
1	2	2014-29-12	GrupoFD	Directorio CODE100	Aprobación para presentación
1	3	2014-29-12	GrupoFD	Directorio CODE100	Aprobación para presentación
1	4	2014-28-04	GrupoFD	Directorio CODE100	Adecuación Procedimiento Emisión

INDICE

1. INTRODUCCIÓN

1.1. Descripción general

El presente documento es la Política de Certificación de CODE100 S. A. (en adelante "CP") 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. 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.

Los certificados digitales emitidos por la CA Raíz y por CODE100 se rigen y ajustan a la Política de Certificación (CP) de la AC Raíz de Paraguay, cuyo cumplimiento es de carácter obligatorio.

La CP fue elaborada conforme a las recomendaciones establecidas en el RFC 3647 'INTERNET X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework"; y contiene los principios y reglas relativos a la gestión de Certificados Digitales, las normas mínimas y básicas que debe cumplir el PSC, el uso de los certificados digitales, entre otras cuestiones relacionadas con la PKI Paraguay.

En resumen, esta CP es específicamente aplicable a:

- Prestador de Servicios de Certificación CODE100 S.A. como CA
- Las Autoridades de Registro.
- Los Solicitantes y Suscriptores de certificados digitales,
- Usuario Final, y
- Parte que confía.

La Habilitación de la CA CODE100 S.A., será aprobada por resolución ministerial, previo dictamen de la DGFD&CE, al igual que la revocación de su habilitación.

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

Esta política contempla los siguientes tipos de certificados:

- Certificado de persona física para autenticación
- Certificado de persona física para firma digital
- Certificado de persona jurídica para autenticación

- Certificado de persona jurídica para firma digital

El PSC, una vez habilitado, pasa a ser parte de la cadena de confianza de la PKI Paraguay, y debe contar con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera una estructura jerárquica.

1.2. Nombre e Identificación del documento

Nombre:	Política de Certificación de CODE100 S.A.
Versión:	1.4
Fecha de aprobación:	28/04/2015
Sitio de internet oficial:	www.code100.com.py
Lugar:	República del Paraguay

1.3. Participantes de la PKI

1.3.1. Autoridades Certificadoras (CA)

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

- Autoridad de Certificación Raíz de la PKI Paraguay
- Prestador de Servicios de Certificación (PSC)

1.3.2. RA (RA)

La RA ejecuta labores de identificación y autenticación de los solicitantes de un Certificado. La misma, debe validar los requisitos de identificación del solicitante, dependiendo del tipo de Certificado y de la especificación de la Política pertinente. Además, tramita las Solicitudes de Revocación de Certificados y valida la información contenida en las solicitudes de certificados.

CODE100 S.A. podrá establecer sucursales en todo el territorio de la república respecto a las funciones de Registro bajo su responsabilidad, cumpliendo las normas y procedimientos establecidos en la normativa vigente, previa comunicación y autorización del Ministerio Industria y Comercio (MIC), en su carácter de Autoridad de Aplicación de la Infraestructura de Clave Pública del Paraguay.

Las Autoridades de Registro habilitadas se publicarán en el sitio:

http://www.code100.com.py/autoridades-de-registro.html

La información relacionada con las Organizaciones que adopten la utilización de certificados digitales emitidos por la AC de CODE100 S.A. en los términos de esta CP, se publicará en el sitio:

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

1.3.3. Suscriptores

En relación a 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 CP y CPS así como de la normativa vigente.

1.3.4. Parte que confía

Es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.5. Otros participantes

Sin estipulaciones.

1.4. Uso del Certificado

1.4.1 Usos apropiados del Certificado

Tipo	Descripción de uso apropiado
Certificado de PSC	Firma de certificado a sus suscriptores. Firma de CRL. • Firma de Certificado (CertificateSigning) • Firma de CRL (CRL Signing)
Certificado de persona física para firma digital	Firma digital • No repudio (Non-Repudiation)
Certificado de persona física para autenticación	Autenticación

	• Firma Digital (Digital Signature) • Cifrado de Clave (Key Encipherment)
Certificado de persona jurídica para firma digital	Firma digital • No Repudio (Non-Repudiation)
Certificado de persona jurídica para autenticación	Autenticación • Firma Digital (Digital Signature) • Cifrado de Clave (Key Encipherment) • Acuerdo de Clave (Key Agreement)

1.4.2. Usos prohibidos del certificado

Los certificados emitidos deben ser utilizados dentro del marco de la normativa vigente que rige la materia.

Cualquier otro uso de los certificados no especificado en esta CP y en la normativa vigente, está fuera del alcance y responsabilidad de esta CP.

El uso indebido de los certificados será sancionado por la CA, pudiendo llegar a la revocación del mismo.

1.5 Administración de la Política

1.5.1. Organización que administra el documento

Nombre: CODE100 S.A.

Dirección: Asunción, Paraguay

Teléfono: (+595) (21) 444789

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

Página Web: www.code100.com.py

1.5.2. Persona de Contacto

Nombre: Carlos E. M. Dossetti

Dirección: Asunción, Paraguay

Teléfono: (+595) (21) 444789

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 Declaración de Prácticas de Certificación (CPS) de la PKI y de los PSC que deseen formar parte de la PKI Paraguay.

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

El Directorio y personal autorizado de CODE100 aprueba el contenido de las Política de Certificación y sus posteriores enmiendas y modificaciones. El MIC aprueba en forma definitiva por resolución la CP de la infraestructura de clave pública del paraguay y la habilitación del PSC.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

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

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

Autoridad de Aplicación (AA): Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente de la Subsecretaría de Estado de Comercio. Órgano Regulador competente designado por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 "De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico".

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

Autoridad Certificadora Raíz (CA Raíz): Es la Autoridad de Certificación Raíz de la PKI Paraguay, cuya función principal es habilitar al PSC y emitirle certificados digitales. Posee un certificado auto firmado y es a partir de allí, donde comienza la cadena de confianza.

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

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

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

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

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

Clave Pública: Es la otra clave del sistema de criptografía asimétrica, que es usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

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

Datos de activación: Valores de los datos, distintos a las claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

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

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

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

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

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

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

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

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

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

Identificador de Objeto (OID): Serie única de números enteros, que identifica inequívocamente un objeto de información.

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

Integridad: Característica que indica que un mensaje de datos o un documentos electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Lista de certificados revocados (CRL): Lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

Módulo criptográfico: Software o Hardware criptográfico que genera y almacena claves criptográficas.

Módulo de Seguridad de Hardware (HSM, Hardware Security Module): Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

No Repudio: Refiere que la posesión de un documento electrónico y la firma digital asociada al mismo, será prueba efectiva del contenido y del autor del documento.

Par de claves: Son las claves privada y pública de un 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#10 (Certification Request Syntax Standard): Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

Parte que confía: Es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos bajo la PKI Paraguay.

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

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

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

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

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

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

Prestador de Servicios de Certificación (PSC): Entidad habilitada ante la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz y solo podrá emitir certificados a usuarios finales.

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

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

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

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

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

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

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

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

Validez de la firma: Aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado.

Verificación de la firma: Determinación y validación de: a) que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

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

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

1.6.2 Acrónimos

Acrónimo / Descripción

C: País (del inglés, Country)

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

CA Raíz: Raíz Autoridad Certificadora Raíz del Paraguay

CI: Cédula de identidad

CIE: Cédula de identidad extranjera

CN: Nombre común (del inglés, Common Name)

CP: Políticas de Certificación (CP por sus siglas en inglés Certificate Policy)

CPS: Declaración de Prácticas de Certificación (CPS por sus siglas en inglés Certification Practice Statement)

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 de la Subsecretaría de Estado de Comercio.

DNS: Servicio de nombre de dominio (DNS por sus siglas en inglés Domaine Name server)

ETSI: Instituto Europeo de Normas de Telecomunicaciones (ETSI por sus siglas en inglés European Telecomunications Standards Institute)

FIPS: Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés Federal Information Processing Standards).

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

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

MIC: Ministerio de Industria y Comercio O Organización (del inglés Organization)

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

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

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

PKI: Infraestructura de Clave Pública (PKI por sus siglas en inglés Public Key Infrastructure).

PSC: Prestador de Servicios de Certificación

PY: Paraguay

RA: RA (RA por sus siglas en inglés Registration Authority).

RFC: Petición de Comentarios (RFC por sus siglas en inglés Request for Comments)

RUC: Registro único del Contribuyente

SN: Número de Serie (del inglés, Serial Number)

SSL: Capa de Conexión Segura (SSL por sus siglas en inglés Secure Sockets Layer)

SMS: Sitio de Máxima Seguridad.

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

2. RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

2.1. Repositorios

EL PSC, es responsable de las funciones de Repositorio para su propia CA y, debe publicar la Lista de Certificados Revocados de sus suscriptores.

Los repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por CODE100 S.A.

2.2 Publicación de Información de Certificación

La publicación de información del CA CODE100 S.A. se realiza en sus servidores, y se puede encontrar en el sitio web identificado como:

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

Se mantiene el repositorio en línea accesible durante las 24hs, los 7 días de la semana, donde se publican las versiones vigentes de los siguientes documentos:

- CP de CODE100
- CPS de CODE100.
- Certificado de la CA Raíz de Paraguay.
- Certificado de la CA CODE100.
- Lista de Certificados Revocados.
- Acuerdo con Suscriptores.
- Las Resoluciones que Habilitan, Suspenden o Revocan al PSC.
- La información relevante de la última auditoría que hubiere sido objeto.
- Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay.
- Identificación, domicilio y medios de contacto.

2.3 Tiempo o frecuencia de Publicación

Cuando se produzca una actualización de los documentos relacionados con el marco legal u operativo del PSC, la nueva versión de los documentos mencionados en el punto "2.2. Publicación de Información del Certificador", se publicará de acuerdo a lo establecido en el punto 9.12 de esta CP.

Salvo comunicación en contrario, los certificados ya emitidos continuarán rigiéndose por los documentos vigentes al tiempo de su emisión. Si el cambio resultare de naturaleza tal que torne inviable la continuidad del uso de esos certificados, CODE100 S.A. lo comunicará a todos sus suscriptores.

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

2.4 Controles de Acceso a los Repositorios

CODE100 S.A. garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio. No se establecen restricciones al acceso a los sitios de publicación de documentación citada en el punto "2.2 Publicación de Información de Certificación", pero CODE100 S.A. establece controles de seguridad para prevenir que personas no autorizadas agreguen o modifiquen información de los repositorios.

3. IDENTIFICACION Y AUTENTICACION

3.1. Registro Inicial

CODE100 S.A. en su sitio web

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

Pone a disposición del Solicitante de un certificado digital, la siguiente información:

a) Las condiciones de utilización del certificado digital;

b) Las características del certificado digital solicitado;

c) Las limitaciones a la responsabilidad;

d) Los procedimientos relacionados a las operaciones vinculadas;

e) Los efectos de la revocación de su propio certificado digital y de la licencia que le otorga la AA;

f) Las obligaciones que el suscriptor asume como usuario del servicio de certificación;

g) Los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta de mal funcionamiento del sistema, o bien presentar reclamos;

La generación del par de clave correspondiente al certificado será implementada en un dispositivo criptográfico provisto por el Solicitante, conforme con la lista de dispositivos criptográficos homologados por CODE100 S.A. publicada en

http://www.code100.com.py/dispositivos-homologados.html

En caso de contar el solicitante con un dispositivo criptográfico propio deberá colocarlo al inicio de la sesión.

La aplicación le mostrará un formulario de Solicitud y deberá ser completado por el solicitante en este mismo formulario. Finalizado el ingreso, el Solicitante confirmará todos los datos proporcionados. Luego, seleccionará la RA para su identificación.

Habiendo confirmado los datos de la solicitud y elegido donde realizar la identificación. El Solicitante procederá a solicitar la elección del proveedor criptográfico con el que se generará el par de claves criptográficas asimétricas. Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. El Solicitante utilizará un dispositivo criptográfico para realizar la generación en el mismo.

Generadas las claves, la aplicación del PSC valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud. El correo incluye: el resumen criptográfico, los datos de la RA elegida, con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, se le informará importe y formas de pago disponibles.

Cuando el Solicitante se presenta para su identificación ante el oficial de registro con toda la documentación exigida, procede a firmar el Acuerdo con Suscriptores.

La aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de la verificación de la identidad del Solicitante y al cumplimiento de los requisitos específicos en relación a las características del tipo de certificado digital solicitado.

El Oficial de Registro, podrá denegar o condicionar la aprobación de la solicitud del interesado hasta el efectivo cumplimiento de los requisitos y condiciones establecidos.

La solicitud para la que no se haya completado el proceso de identificación, caducará a los treinta (30) días de generada.

Una vez identificado el Solicitante y aprobada la solicitud por el Oficial de Registro, la aplicación de la CA emitirá el certificado. El Solicitante descargará e instalará el certificado solicitado.

3.1.1. Tipos de Nombres

En la sección 3.1.4 se explican las reglas para interpretación del código de identificación. El uso del campo número de serie (serial number OID 2.5.4.5) se establece como un Campo del nombre distintivo del sujeto. En concordancia a lo definido en la familia de estándares X.501

A continuación se presentan los formatos de los nombres para el suscriptor del certificado dependiendo de su tipo.

En el caso de la CA de PSC CODE100

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	CODE100 S.A.	Denominación o Razón Social de la Persona Jurídica habilitada como PSC
Common Name (CN)	CA – CODE100	CA + Nombre de la CA
Serial Number {OID: 2.5.4.5}	RUC 80080610-7	RUC Número de Cédula Tributaria correspondiente a CODE100

En el caso del Suscriptor Persona Física

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	JUAN PEREZ GOMEZ	Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes.
Organization Unit (OU)	PERSONA FISICA	La Política identifica si se trata de un certificado para: Persona física o Persona jurídica.

Common Name (CN)	JUAN PEREZ GOMEZ FIRMA/AUTENTICACION	Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes. El propósito debe ser FIRMA o AUTENTICACION
Serial Number {OID: 2.5.4.5}	CI 9999999	CI más Número de Cédula de Identidad para paraguayos o CIE más Cédula de identidad para extranjeros
Surname (SN) {OID: 2.5.4.4}	PEREZ GOMEZ	Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes.
GivenName (G) {OID:2.5.4.42}	JUAN	Se registra el nombre de suscriptor, en mayúsculas y sin Tildes

En el caso del Suscriptor Persona Jurídica

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	EMPRESA S.A.	Razón Social de la entidad, según inscripción en el Registro Público, en mayúsculas y sin tildes.
Organization Unit (OU)	PERSONA JURIDICA	Identifica si se trata de un certificado para: Persona física o Persona jurídica
Common Name	EMPRESA S.A. FIRMA/AUTENTICACION	Nombre del Suscriptor en mayúsculas y sin tildes o nombres de dominio de la organización. El propósito debe ser FIRMA o AUTENTICACION

Serial Number {OID: 2.5.4.5}	RUC 99999999-9	RUC Número de Cédula Tributaria correspondiente al suscriptor Debe ser validada durante el proceso de registro
Subject alternative name	DNS=www.EMPRESASA.com.py	Este es un valor opcional donde pueden colocarse otros nombres de dominio, direcciones de correo electrónico, direcciones IP, u otros identificadores únicos. Este campo se aplica únicamente para los certificados de AUTENTICACION

3.1.2. Necesidad de Nombres significativos

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

3.1.3. Anonimato o seudónimos de los suscriptores

A fin de dar cumplimiento efectivo al atributo de No Repudio característico de los Certificados de Firma Digital no se admite el anonimato. Asimismo, el Seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del Certificado.

3.1.4. Reglas para interpretación de varias formas de Nombres

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

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	RUC 99999999-9

Certificado de Persona física para firma digital y para autenticación

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

Tipo de Documento	Prefijo	Formato
Cédula de identidad CI	CI	CI 9999999
Cédula de identidad para extranjero	CIE	CIE 99999999

3.1.5. Unicidad de los nombres

La CA debe asegurar que el "nombre distintivo del suscriptor" (subject distinguished name) es único dentro de la jerarquía PKI Paraguay.

Al respecto, CODE100 S.A. se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre en los certificados de sus suscriptores.

El procedimiento para la resolución de homonimias se basa en la utilización de la cedula tributaria (RUC) en las Personas Jurídicas y de la Cedula de Identidad (CI) o Cedula de Identidad de Extranjeros (CIE) en la Personas Físicas.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros. En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

La PKI Paraguay no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas o instituciones y marcas registradas.

La CA 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 de la CA.

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 DGFD&CE., en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 Autenticación de identidad de Persona Jurídica

El PSC, en su función de RA debe validar la identidad de la empresa o institución solicitante. Como mínimo, se debe recabar el nombre o razón social, el RUC y los datos del representante legal debidamente acreditado. Posteriormente, la RA debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes.

En el Certificado de Personas Jurídicas para autenticación, si el solicitante requiere incluir uno o más nombres de Dominio en el campo ‘’Nombre alternativo del Sujeto” (Subject alternative name). CODE100 S.A., debe verificar la información de dominio suministrada por el solicitante, contra los datos oficiales correspondientes.

3.2.3 Autenticación de identidad de Persona Física

El Proceso de autenticación de la identidad del solicitante del Certificado debe ser en forma presencial, para el efecto, el PSC en su función de RA debe verificar la validez y la vigencia de los documentos presentados. Posteriormente, éste debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.4 Información del Suscriptor no verificada

No aplica.

3.2.5. Validación de la Autoridad (Capacidad de hecho)

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

En el caso de Certificados de Personas Físicas, debe validar:

- 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.

El PSC, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.6. Criterios para interoperabilidad

Podrán ser reconocidos los Certificados Digitales Extranjeros de conformidad a la normativa vigente.

3.3. Generación de nuevo par de claves después de una revocación - Sin compromiso de clave

En caso de que el Suscriptor requiriera generar un nuevo par de claves después de una revocación, deberá realizar el proceso de Solicitud completo y la presentación frente al Oficial de Registro para validar su identidad.

3.4. Requerimiento de revocación

La revocación podrá ser iniciada por el Suscriptor, por la RA o por la CA.

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 la CA debe procesar la Solicitud de revocación.

El Suscriptor que inicia la revocación se debe identificar en el portal con su N° de RUC (Personas jurídicas) N° de CI o N° de CIE (personas físicas) y luego con su Pin de revocación, obtenido durante el proceso de Solicitud, inicia el proceso de revocación de certificado.

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.

La RA o la CA podrán iniciar de oficio o por decisión del responsable de CODE100 S.A., la revocación de certificados, según lo indicado en el "4.9.1. Circunstancias para la revocación".

La RA o la CA, con la documentación relacionada con la revocación, procede a ingresar a la aplicación del PSC con su clave, selecciona el certificado a revocar que le pertenece al suscriptor e inicia, con su solicitud, el proceso automático de revocación. Deja asentado en los registros informáticos de la RA la revocación efectuada.

Los suscriptores se encuentran obligados a: 1) notificar a la RA de toda modificación de la situación del suscriptor que llevaría a inhabilitarlo como suscriptor de un certificado conforme a la presente CP, o bien la modificación de los datos del suscriptor que llevarían a modificar la información contenida en el certificado expedido a favor de dicho suscriptor y 2) solicitar el requerimiento de revocación inmediata del certificado.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de certificado

4.1.1. Quién puede presentar una solicitud de certificado

En la siguiente lista se detallan las personas que pueden presentar una solicitud de certificado:

- Para el caso de certificado de persona física, cualquier 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 apoderado con poder suficiente.

4.1.2 Proceso de Inscripción y responsabilidades

El solicitante tiene las siguientes responsabilidades dependiendo del tipo de certificado:

4.1.2.1 Certificado de Persona Física para firma digital y para autenticación

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el Solicitante, quien debe acreditar fehacientemente su identidad.

Para poder efectuar la Solicitud de un certificado, el Solicitante debe:

- Ingresar al portal del Suscriptor.
- Contar con su dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado.
- Cumplir con los requisitos mínimos de configuración de hardware y software.
- Contar con un dispositivo criptográfico propio, de los modelos homologados por el PSC y deberá colocarlo al inicio de la sesión.
- La aplicación, mostrara el formulario de Solicitud de persona física, este deberá ser completado por el solicitante.
- Completados los datos de la Solicitud, el Solicitante deberá confirmarlos.
- El sistema a continuación desplegará las RA, debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10.
- Generadas las claves, la aplicación del PSC valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.

- El correo incluye: la Solicitud con el resumen criptográfico (huella MD5), los datos de la RA con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, en los casos que corresponda se le informará importe y formas de pago disponibles.
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.
- Cumpliendo el Solicitante podrá presentarse en la RA elegida o ser visitado por un Oficial de Registro para su identificación, la aprobación de la Solicitud de certificado digital estará sujeta a cubrir los requerimientos para la verificación de la identidad del Solicitante y los requisitos específicos en relación con las características del certificado digital solicitado.
- En caso de ser visitado por un Oficial de Registro, este deberá validad que la generación del requerimiento del certificado de firma digital sea realizada en un dispositivo criptográfico homologado por CODE100 S.A.
- Luego de aprobada de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

4.1.2.2 Certificado de Persona Jurídica para firma digital y para autenticación

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el representante legal, administrador o apoderado de la persona jurídica Solicitante, quien luego deberá acreditar fehacientemente su identidad.

Para poder efectuar la solicitud de un certificado, el Solicitante debe:

- El Solicitante deberá ingresar al portal del Suscriptor.
- Contar con su dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado.
- Cumplir con los requisitos mínimos de configuración de hardware y software.
- En caso de contar el Solicitante con un dispositivo criptográfico propio, de los modelos homologados por el PSC, deberá colocarlo al inicio de la sesión.
- El proceso de solicitud podrá ser iniciado solamente por el apoderado, administrador o representante legal de la persona jurídica a favor de la cual se emitirá el certificado, y será asignado por la aplicación en función de los datos del Solicitante.

- Completados los datos de la Solicitud, el Solicitante deberá confirmarlos.
- El sistema a continuación desplegará las Autoridades de Registro debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10.
- Generadas las claves, la aplicación del PSC valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.
- El correo incluye: la Solicitud con el resumen criptográfico (huella MD5), los datos de la RA con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, en los casos que corresponda se le informará importe y formas de pago disponibles.
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.
- Cumpliendo el Solicitante con presentarse en la RA elegida o ser visitado por un Oficial de Registro para su identificación, la aprobación de la Solicitud de certificado digital estará sujeta a cubrir los requerimientos para la verificación de la identidad del Solicitante y los requisitos específicos en relación con las características del certificado digital solicitado.
- En caso de ser visitado por un Oficial de Registro, este deberá validad que la generación del requerimiento del certificado digital sea realizada en un dispositivo criptográfico homologado por CODE100 S.A.
- Luego de aprobada de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

4.2. Procesamiento de la Solicitud del Certificado

4.2.1 Ejecución de las funciones de Identificación y Autenticación

Certificado de Persona Física o de Persona Jurídica

La encargada de estas funciones es la RA, entidad que debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el punto "3.2. Validación inicial de identidad".

4.2.2 Aprobación o rechazo de solicitudes de certificado

Certificado de Persona Física o Jurídica

La RA debe rechazar la solicitud de certificado en los casos que no se de cumplimiento a la normativa vigente y a lo establecido en esta política.

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 CPS.

4.3. Emisión del Certificado

Cumplidos los recaudos del proceso de identificación y autenticación de acuerdo con esta CP, y una vez aprobada la Solicitud por la RA, la CA emite el correspondiente certificado, firmándolo digitalmente con su clave privada.

El sistema pone el certificado en el Portal del Suscriptor, a disposición de su titular y le comunica esa disponibilidad por correo electrónico. El Portal del Suscriptor se encuentra en:

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

En este sitio web cada Solicitante puede acceder únicamente a su propia información.

4.3.1 Acciones de la CA durante la emisión de los certificados

Una vez ejecutadas las labores de identificación y autenticación de los solicitantes, la RA debe verificar que el solicitante cumpla con los requisitos establecidos en esta CP, con las normas técnicas y legislación vigente que rige la materia.

La emisión de un certificado implica, la realización de las siguientes acciones por parte de la CA:

- Asegurarse que la generación de un par de claves y un certificado se haya realizado de manera segura de acuerdo a la sección "3.2.1. Métodos para comprobar la posesión de la clave privada"
- Asociación del par de claves que corresponde al certificado con un suscriptor, y que el par de claves se encuentre en su posesión.
- Emisión del certificado digital para su uso operativo, de acuerdo con el Nombre Distintivo asociado con el suscriptor.

4.3.2 Notificación al suscriptor sobre la emisión del Certificado Digital

Luego de emitido el certificado digital la CA debe notificar al suscriptor la emisión del mismo.

Esta notificación no será requerida en el caso que el certificado digital sea emitido en la infraestructura tecnológica de la RA, en presencia del suscriptor en un dispositivo de seguridad criptográfico. De este modo el certificado digital y las claves se encuentren en posesión del suscriptor desde su emisión o generación.

En el caso en que la emisión no sea en forma presencial el PSC notificará al suscriptor por medios electrónicos que se ha creado el certificado digital, que se encuentra disponible y la forma de obtenerlo.

4.4. Aceptación del Certificado

4.4.1 Conducta constitutiva de aceptación de certificado

Certificado de Persona física y Jurídica

Una vez notificado de la emisión de un certificado a su nombre, el Suscriptor o bien su representante legal o apoderado en caso de tratarse de certificados de personas jurídicas, deberá controlar su contenido y descargar el certificado desde el Portal del Suscriptor.

En caso de que existiera algún error u omisión en los datos del suscriptor contenidos en el certificado, deberá revocarlo con su PIN de revocación desde el Portal del Suscriptor.

En caso de formular un reclamo de no aceptación del certificado antes de descargar el mismo deberá realizarlo dentro de las 48 horas de la notificación de CODE100 S.A. de la puesta a disposición en el portal del suscriptor del certificado a su nombre.

Ante la ausencia de reclamos a la RA por parte del Suscriptor, en cuanto a los datos del certificado, se acepta la exactitud del contenido del certificado desde el momento de su notificación y el Suscriptor asume la totalidad de las obligaciones y responsabilidades establecidas por esta CP.

4.4.2 Publicación del Certificado por la CA

La CA no debe publicar información de los certificados emitidos en los repositorios de acceso público.

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

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

4.5 Uso del par de claves y del certificado

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

El uso de la clave privada correspondiente a la clave pública, contenida en el certificado, solamente debe ser permitido una vez que el suscriptor haya aceptado el certificado emitido, dicho uso, debe realizarse conforme a la normativa vigente, lo estipulado en esta CP y el acuerdo de suscriptores respectivo.

Los suscriptores deben proteger su clave privada del uso no autorizado y una vez expirado o revocado el certificado, su uso queda expresamente prohibido.

Notificar a la CA sin dilación indebida:

- La pérdida, robo o extravío del dispositivo criptográfico,
- El compromiso potencial de su clave privada,
- La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa,
- Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera contener el suscriptor.

Certificado de PSC

La Clave privada y el certificado del PSC podrá ser utilizado con el único propósito de:

- Firmar los certificados personas físicas y jurídicas para firma digital y para autenticación; y,
- Firmar las Listas de Certificados Revocados (CRL) correspondientes.

Certificado de persona física para autenticación y firma digital

El uso de los certificados emitidos por el PSC, debe ser acorde a lo dispuesto en el punto "6.1.7. Propósito de usos de clave (Campo key usage x509 v3)" de la presente CP.

Certificado de persona jurídica para autenticación y firma digital

Los certificados de persona jurídica para firma digital serán usados de conformidad a lo establecido en la normativa vigente.

En el caso que el titular del certificado sea una persona jurídica, serán responsables por el uso sus representantes o personas designadas.

Cada persona jurídica deberá desarrollar y establecer los mecanismos de seguridad informática y de infraestructura física, así como los reglamentos, procedimientos o políticas que considere pertinentes para resguardar y delimitar el uso de dicho certificado en su organización.

El uso de los certificados emitidos por el PSC, debe ser acorde a lo dispuesto en el punto "6.1.7. Propósito de usos de clave (Campo key usage x509 v3)" de la presente CP.

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

La parte que confía debe aceptar las estipulaciones establecidas en la presente CP, en todo lo que les resulte aplicable, como condición indispensable para confiar en el certificado.

Antes de cualquier acto de confianza la parte que confía debe evaluar en forma independiente:

- Que el certificado sea utilizado para un propósito apropiado, y que no esté prohibido o restringido por la presente CP. El PSC no es responsable de esta tarea.
- El estado del certificado y el estado de todPos los certificados de las CA en la cadena que emitieron los certificados.

4.6 Renovación del certificado

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

4.7 Re-emisión de claves de certificado

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

4.7.1 Circunstancias para re-emisión de claves de certificado

No aplica.

4.7.2 Quien puede solicitar la certificación de una clave pública

No aplica.

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

No aplica.

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

No aplica.

4.7.5 Conducta constitutiva de aceptación de un certificado re-emitido

No aplica.

4.7.6 Publicación por la CA de los certificados re-emitidos

No aplica.

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

No aplica.

4.8 Modificación de certificados

4.8.1 Circunstancias para modificación del certificado

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 la CA de los Certificados modificados

No aplica.

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

No aplica.

4.9 Revocación y suspensión

4.9.1 Circunstancias para la revocación

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

La CA revocará un certificado por ella emitido, en los casos en que:

- Lo solicite el titular del certificado por cualquier causa, incluida el haber tomado conocimiento de que su clave privada esté comprometida y haya dejado de ser segura.
- CODE100 S.A. determine que el certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
- CODE100 S.A. determine que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Fuere solicitado por resolución judicial o de la AA de la Ley debidamente fundada.
- CODE100 S.A. determine que el certificado dejó de cumplir con las políticas y normas legales y reglamentarias.
- Por fallecimiento del titular, declaración judicial de ausencia con presunción de fallecimiento o declaración judicial de incapacidad, en el caso de persona física comunicada fehacientemente por sus herederos o autoridad judicial competente a CODE100 S.A.
- Por cese del representante legal y su sustituto, en el caso de personas jurídicas comunicada fehacientemente por el nuevo representante legal, administrador o apoderado de la persona jurídica a CODE100 S.A.
- Por cambio en los atributos de un certificado, aun cuando hubieran sido válidos al tiempo de su emisión.
- Por cese de la existencia de la Persona Jurídica, comunicada fehacientemente por el representante legal de la misma a CODE100 S.A.
- Por cese de la Licencia del PSC.
- Insolvencia, liquidación, quiebra de una persona jurídica.
- Cuando finaliza el acuerdo de suscriptor con el PSC, por cumplirse la vigencia del mismo o por voluntad propia del suscriptor.

4.9.2 Quien puede solicitar Revocación

Los habilitados para realizar la solicitud de revocación son:

- El Suscriptor del certificado, si se trata de una persona física.
- El representante legal, administrador o apoderado, si se trata de una persona jurídica.
- La RA.

- La Autoridad de Aplicación.
- La Autoridad Judicial competente.
- El PSC.
- Además, cualquier persona puede solicitar la revocación de un certificado ante la CA correspondiente presentando evidencia contundente del uso indebido del certificado, compromiso de la clave, fallecimiento del titular u otro motivo de revocación establecido en la normativa vigente y esta CP.

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.

Las RA conservarán como documentación probatoria toda solicitud de revocación y el material probatorio vinculado. Se registraran en los registros informáticos de la RA la revocación.

Los suscriptores o sus representantes serán notificados en sus respectivas direcciones de correo electrónico del cumplimiento del proceso de revocación.

La revocación se reflejará en la próxima Lista de Certificados Revocados, cuando sea generada de acuerdo con lo especificado en el punto "4.9.7 Frecuencia de emisión de la CRL".

La RA debe evaluar la solicitud de revocación presentada y verificar que la misma ha sido presentada por el suscriptor del certificado, por una autoridad competente o un tercero de acuerdo con la sección "3.4 Requerimiento de revocación".

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

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

4.9.4 Periodo de gracia para solicitud de revocación

No se estipulan periodo de gracia para revocación de certificados.

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

La recepción de la solicitud de revocación está disponible 7 días de la semana x 24 hs. a través de la aplicación del PSC desde:

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

Esta solicitud será procesada de inmediato, sin intervención de la RA.

En caso de que el Suscriptor se presente personalmente ante la RA, la solicitud de revocación será ingresada por el Oficial de Registro y también procesada de inmediato.

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 las 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 la CA.

4.9.7 Frecuencia de Emisión del CRL

La CA CODE100 S.A. genera y publica periódicamente una única lista conteniendo todos los certificados revocados por ella, en forma acumulativa, en formato del CRL X.509 v2, sin superar las veinticuatro (24) horas entre publicaciones. Además cuando surja la revocación del certificado de un Suscriptor, la CA CODE100 S.A. generará y publicará una nueva CRL.

4.9.8 Latencia máxima para CRLs

La CA debe publicar la CRL en el repositorio en un plazo no mayor a una hora posterior a su generación.

4.9.9 Disponibilidad de verificación de revocación/ estado en línea

Toda CA debe mantener disponible un repositorio con información del estado de los certificados emitidos, el cual puede ser accedido vía web. Adicionalmente, la CA debe implementar el servicio de validación en línea OCSP.

4.9.10 Requerimientos para verificar la revocación en línea

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

4.9.11 Otras formas de advertencias de revocación disponibles

Sin estipulaciones.

4.9.12 Requerimientos especiales por compromiso de clave privada

El PSC, 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.

En todas las situaciones que involucren el compromiso de la clave privada del Suscriptor, éste deberá revocar su certificado. Podrá hacerlo por alguna de las vías indicadas en el punto "3.4. Requerimiento de revocación".

4.9.13 Circunstancias para suspensión

Según la normativa no se aplica la suspensión del Certificado.

4.9.14 Quien puede solicitar la suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del período de suspensión

No aplica.

4.10 Servicios de comprobación de estado de Certificado

4.10.1 Características operacionales

El estado de los certificados debe estar disponible a través de los CRL publicados en un sitio principal de internet (en el URL especificado en el CP) y para los PSC, es obligatorio implementar un servicio OCSP.

4.10.2 Disponibilidad del Servicio

Los sistemas de distribución de CRLs y de consulta en línea del estado de los certificados deberán estar disponibles 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

La CA no debe custodiar claves de los suscriptores de ningún certificado, únicamente se mantienen respaldos de sus propias claves privadas de acuerdo con el "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio".

Para los efectos del "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio", las claves privadas de las CA deben estar en custodia y respaldadas 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

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

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

La infraestructura tecnológica de la CA, se encuentra situada dentro del territorio paraguayo, y no utiliza una infraestructura tecnológica establecida en el extranjero.

Las operaciones de la CA, se realizan dentro de un ambiente de protección física que impide y previene usos o accesos no autorizados o divulgación de información sensible.

Las instalaciones de la CA cuentan con seis perímetros de seguridad física:

- Primer perímetro: acceso a las instalaciones de la CA.
- Segundo perímetro: acceso al área de procesos administrativos de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el primero.
- Tercer perímetro: acceso al área de operación de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo.
- Cuarto perímetro: acceso al área de operaciones críticas de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el tercero.
- Quinto perímetro: acceso al área de resguardo de documentos y dispositivos sensibles. Área interna al tercer perímetro.
- Sexto perímetro: acceso al área de resguardo de clave privada. Área interna al cuarto perímetro.

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

En el caso que en el periodo de operatividad de CODE100 S.A., éste decida trasladar su infraestructura tecnológica principal y/o alterna a un sitio diferente del autorizado por la CA, se deberá cumplir cuanto sigue:

- Solicitar a la CA Raíz formalmente el traslado de su infraestructura tecnológica habilitada anteriormente, a un sitio que reúna las condiciones establecidas en la CP Vigente.
- La CA Raíz procederá a una inspección extraordinaria del nuevo sitio, a efectos de verificar el cumplimiento de los estándares de seguridad establecido en la CP vigente.
- Aprobada la inspección, CODE100 S.A., procederá al traslado de la infraestructura tecnológica, conforme al procedimiento elaborado por él, con la conformidad de la CA. Si la inspección revelare, alguna anormalidad, el traslado será denegado, pudiendo CODE100 S.A. solicitar una nueva inspección subsanada la irregularidad.
- La CA, designará personal técnico que intervendrá en el proceso de traslado, en especial de la clave privada.

5.1.2 Acceso físico

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

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

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

Para acceder al tercer perímetro de seguridad se requerirá 2 factores de autenticación. Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por, al menos un personal de la CA.

En ésta área se desarrollan actividades como: servicios de soporte, climatización, energía, comunicaciones, monitoreo, entre otras.

Para acceder al cuarto perímetro de seguridad se requerirá 2 factores de autenticación como mínimo (al menos uno de ellos debe ser biométrico). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos irán

acompañados por al menos dos personales de la CA. En ésta área se realizan actividades de emisión y revocación de certificados, emisión de CRL, entre otras.

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

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

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

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

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

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

5.1.3 Energía y Aire acondicionado

El equipo de la CA es protegido contra fallas en el fluido eléctrico corriente y otras anomalías en la energía, las instalaciones son equipadas con sistemas de energía primario y de respaldo para asegurar continuidad del fluido eléctrico.

Las instalaciones cuentan con sistemas de aire acondicionado de precisión redundantes.

El equipo instalado para climatizar el recinto, es capaz de controlar la humedad relativa del mismo.

5.1.4 Exposiciones al agua

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

5.1.5 Prevención y protección contra fuego

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

5.1.6 Almacenamiento de medios

La CA asegura el adecuado manejo y protección de los medios de almacenamiento de información, que contiene datos críticos o sensitivos del sistema, contra daños accidentales (agua, fuego, electromagnetismo) e impide, detecta y previene su uso no autorizado, acceso o su divulgación.

5.1.7 Eliminación de residuos

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

5.1.8 Respaldo fuera de sitio

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

Las copias de seguridad externas son establecidas y mantenidas de conformidad con la "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio" de manera compatible con los estándares internacionales.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Las personas designadas para gestionar la infraestructura de la CA asumen "Roles de Confianza" para la asignación de los mismos, se considera la contraposición de intereses.

Los Roles contemplan, al menos las siguientes responsabilidades:

a) Responsabilidad general de administrar la implementación de las prácticas de seguridad de la CA (Coordinador de Seguridad);

b) Aprobación de la emisión y revocación de los certificados (Jefe de Área);

c) Instalación, configuración y mantenimiento de los sistemas de la CA (Administrador de Sistemas);

d) Operación diaria de los sistemas de la CA, respaldo y recuperación de sistemas (Responsable Técnico);

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

f) Funciones de gestión del ciclo de vida de claves criptográficas (ejemplo: custodios de componentes de claves)

g) Desarrollo de sistemas de la CA.

h) Funciones de Gestión de Recursos Humanos del PSC (Responsable de Recursos Humanos);

i) Funciones de Asesoramiento Legal, Administración de Contratos (Responsable Legal);

j) Coordinar tareas tras la declaración de una Contingencia, verificación de mantenimiento y actualización del Plan de Contingencia (Responsable de Contingencia)

5.2.2 Número de personas requeridas por tarea

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

5.2.3 Identificación y autenticación para cada rol

La CA confirma la identidad y autorización de todo el personal que intente iniciar labores de confianza. La autenticación de la identidad incluye la presencia física de la persona y una verificación por medio de documentos vigentes de identificación legalmente reconocidos.

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:

- La validación de información en aplicaciones de certificado y de solicitudes o información del suscriptor.
- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación.
- La emisión o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La emisión o destrucción de los certificados de la CA.
- La puesta en operación de la CA en producción.
- La auditoría interna de la operación de la CA debe ser ejecutada por un rol particular.

5.3 Controles de personal

Los controles de seguridad del personal que desempeñan los roles en el PSC, serán los establecidos por CODE100 S.A. e implementados a través de su Responsable de Recursos Humanos. CODE100 S.A. realiza una evaluación anual del desempeño de todo su personal.

5.3.1 Requerimientos de experiencia, capacidades y autorización

Las CA suscribe un documento con las personas designadas para desempeñar roles de confianza donde se establece las funciones, obligaciones, responsabilidades y sanciones.

Las personas designadas, además deben:

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

5.3.2 Procedimientos de verificación de antecedentes

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

- Confirmación de empleos anteriores.

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

Para cada persona vinculada con los servicios de certificación, CODE100 S. A. confecciona un legajo de antecedentes laborales, calificaciones profesionales, experiencia e idoneidad.

5.3.3 Requerimientos de capacitación

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

- Operación del software y hardware.
- Políticas y procedimientos organizacionales.
- Procedimientos de seguridad y operacionales.
- Normativa vigente que rige la materia.

5.3.4 Requerimientos y frecuencia de capacitación

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

La CA provee los programas de entrenamiento y actualización a su personal para asegurar que el personal mantiene el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

CODE100 S.A. realiza cursos de entrenamiento e instrucción en las políticas y procedimientos que conforman los manuales operativos de la CA, como así también ante cambios en la tecnología de firma digital o en las plataformas utilizadas.

Conforme se producen cambios en la tecnología de firma digital, en las plataformas utilizadas por la CA o en sus procedimientos, CODE100 S.A. elabora programas de capacitación específicos para todo el personal afectado.

La capacitación será realizada al menos una (1) vez al año, siendo evaluado el personal afectado y otorgándose certificación cuando así correspondiere.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

La CA efectúa una rotación de sus roles de confianza. La frecuencia de la rotación del personal debe ser al menos:

- una vez cada tres años, para CODE100 S.A.

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

5.3.6 Sanciones para acciones no autorizadas

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

5.3.7 Requisitos de contratación a terceros

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

- Existe un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.
- No se posee personal disponible para llenar los roles de confianza.
- Los mismos cumplen con los mismos requisitos del punto "5.3.1 Requerimiento de experiencia, capacidades y autorizaciones".
- Una vez finalizado el servicio contratado se revocan los derechos de acceso.

5.3.8 Documentación suministrada al personal

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

5.4 Procedimiento de Registro de auditoría

El PSC mantiene controles para proveer una seguridad razonable de que:

- Los eventos relacionados con el ambiente de operación de la CA, la gestión de las claves y los certificados, son registrados exacta y apropiadamente;
- Se mantiene la confidencialidad y la integridad de los registros de auditoría vigentes y archivados;

- Los registros de auditoría son archivados completa y confidencialmente;
- Los registros de auditoría son revisados periódicamente por personal autorizado.

La CA mantiene registros de auditoría ("logs") de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros y conservándolos por 10 años como mínimo.

Los registros de auditoría son analizados por un servicio que registra en forma automática las alteraciones en el funcionamiento de la instalación en las tareas de monitoreo habitual del funcionamiento de los sistemas, las aplicaciones y los procesos.

5.4.1 Tipos de eventos registrados

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

Administración del ciclo de vida de las claves criptográficas	a) Generación y almacenamiento de las claves criptográficas del PSC. b) Resguardo y recuperación de las claves criptográficas del PSC. c) Utilización de las claves criptográficas del PSC. d) Archivo de las claves criptográficas del PSC. e) Retiro de servicio de datos relacionados con las claves criptográficas. f) Destrucción de claves criptográficas del PSC. g) Identificación de la entidad que autoriza una operación de administración de claves criptográficas. h) Identificación de la entidad que administra los datos relativos a las claves criptográficas. i) Compromiso de la clave privada.
Administración del ciclo de vida de los certificados	a) Recepción de solicitudes de certificados nueva o renovación. b) Transferencia de claves públicas para la emisión del certificado. c) Cambios en los datos de la solicitud del certificado. d) Generación de certificados. e) Distribución de la clave pública del PSC. f) Solicitudes de revocación de certificados.

	g) Generación y emisión de listas de certificados revocados. h) Acciones tomadas en relación con la expiración de un certificado.
Administración del ciclo de vida de los dispositivos criptográficos	a) Esta actividad estará bajo la responsabilidad del suscriptor. b) El PSC solo registra el uso del dispositivo.
Información relacionada con la solicitud de Certificados	a) Tipos de documentos de identificación presentados por el solicitante. b) Otra información de identificación. c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación. d) Identificación de la entidad que recibe y acepta la solicitud. e) Método utilizado para validar los documentos de identificación. f) Identificación de la RA.
Eventos de seguridad	a) Lecturas y/o escrituras en archivos sensibles de seguridad. b) Borrado de datos sensibles de seguridad. c) Cambios en los perfiles de seguridad. d) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos. e) Caídas del sistema, fallas en el hardware y software, u otras anomalías. f) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad. g) Cambios en la relación entre CODE100 S.A. y personal relacionado con el proceso de certificación. h) Accesos a los componentes del sistema de la CA i) Eventos o situaciones no previstas.

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

5.4.2 Frecuencia de procesamiento del registro

El Administrador de Auditoría realiza al menos una vez al mes revisiones de los registros de auditoría, sin necesidad de previo aviso; mientras que la CA realiza al menos una revisión de los registros cada cuatro meses.

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

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

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

5.4.3 Período de conservación del registro de auditoría

Las CA archiva los registros de auditoría de acuerdo a la sección "5.5.2. Periodos de retención para archivos"

5.4.4 Protección del registro de auditoría

Los registros de auditoría archivados se mantienen de forma de prevenir su revelación, modificación, destrucción no autorizada o cualquier otra intromisión.

5.4.5 Procedimientos de respaldo de registro de auditoría

La CA mantiene copias de respaldo de todos los registros auditados.

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

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

5.4.7 Notificación al sujeto que causa el evento

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

5.4.8 Evaluación de Vulnerabilidades

La CA obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso. Además, se evalúa el riesgo a que se expone la organización ante esas vulnerabilidades y se toman medidas para reducir el impacto.

5.5 Archivos de registros

5.5.1 Tipos de registros archivados

La CA almacena los registros para establecer la validez de una firma y de la operación propia de la infraestructura PKI. Se archivan los siguientes datos:

Durante el inicio de operaciones de la CA:

- La Habilitación del PSC,
- el CP y el CPS;
- Cualquier acuerdo contractual para establecer los límites de la CA;
- La configuración del sistema que requiere la CA.

Durante la operativa de la CA:

- Modificaciones o actualizaciones de cualquiera de los ítems anteriores;
- Solicitudes de certificados o de revocación;
- Documentación para autenticar la identidad del suscriptor;
- Documentación de recepción y aceptación del certificado;
- Documentación de recepción de dispositivos de almacenamiento de claves;
- Todos los certificados y CRL (información de revocación) tanto emitidos o publicados;
- Registros de auditoría;
- Otros datos o aplicaciones para verificar el contenido de los archivos;

5.5.2 Periodos de retención para archivos

Todos los archivos se mantienen por un periodo de al menos diez años. Además de mantener los controles para que los archivos sean revisados durante el periodo de retención definido.

5.5.3 Protección de archivos

Los archivos no son modificados o eliminados por alguna operación no autorizada de la CA.

La misma mantiene la lista de personas autorizadas a mover los registros a otros medios.

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

5.5.4 Procedimientos de respaldo de archivo

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

5.5.5 Requerimientos para sellado de tiempo de registros

No aplica.

5.5.6 Sistema de recolección de archivo (interno o externo)

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

5.5.7 Procedimientos para obtener y verificar la información archivada

Solamente el personal de confianza autorizado está habilitado para obtener acceso al archivo.

La CA realiza pruebas de restauración de la información archivada al menos una vez al año. La integridad de la información es verificada cuando es restaurada.

5.6 Cambio de clave

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

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

Nivel de Jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de Suscriptores	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 PSC	8	10	El Certificado emitido al PSC tiene: 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 la CRL de usuarios o suscriptores.

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 es de al menos el tiempo operacional del certificado de un suscriptor.

Por lo tanto, el certificado anterior puede 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.

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

5.7 Recuperación de desastres y compromiso

5.7.1 Procedimiento para el manejo de incidente y compromiso

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

Las personas designadas que ejecutan roles de confianza velan por la seguridad de las instalaciones y la CA mantiene procedimientos para que los mismos reporten los incidentes.

La CA establece un "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio", que permite el restablecimiento y la continuidad del negocio, y la recuperación frente a desastres. Este plan contempla las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación. Dicho plan, asegura que los aspectos básicos del negocio, tales como: servicios de validación o revocación, puedan ser reasumidos en el menor tiempo posible.

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

El "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio" establece los procedimientos y actividades relacionados con la continuidad del servicio de certificación de firma digital y será de aplicación desde el momento de la declaración de la contingencia hasta la restauración de la operatoria normal.

5.7.2 Corrupción de datos, software y/o recursos computacionales

Posterior a una corrupción de recursos computacionales, software o datos, la CA afectada realiza, en forma oportuna, un reporte del incidente y una respuesta al evento.

5.7.3 Procedimientos de compromiso de clave privada de la entidad

El "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio" considera el compromiso o sospecha de su clave privada como desastre. En este caso, se prevé la revocación del certificado, la publicación y difusión inmediata.

5.7.4 Capacidad de continuidad del negocio después de un desastre

La CA cuenta con un proceso administrativo para desarrollar, probar, implementar y mantener sus planes de continuidad del negocio.

La CA desarrolla, prueba, mantiene e implementa un "Plan de Contingencia, recuperación Frente a Desastres y Continuidad del Negocio" destinado a mitigar los efectos de cualquier desastre natural o producido por el hombre. Los planes de recuperación de desastres se enfocan en la restauración de los servicios de sistemas de información y de las funciones esenciales del negocio.

CODE100 S.A. cuenta con un sitio alterno, con las características necesarias de acuerdo con los estándares de seguridad y las protecciones correspondientes. El acceso al sitio es las 24 horas, los 365 días del año, lo que le permite asegurar la continuidad de sus servicios.

Están previstos mecanismos de prueba y simulación con frecuencia periódica o cuando los cambios realizados al hardware, software de base y/o software aplicativo lo ameriten. Las pruebas del plan tienen por objeto brindar los elementos necesarios para mantener el entrenamiento del personal y minimizar el tiempo de recuperación de la continuidad del negocio.

5.8 Terminación de una CA

El PSC puede cesar en sus actividades. Este hecho se podrá producir a partir de la manifestación del Directorio de CODE100 S.A., como máxima autoridad de la empresa, sobre su decisión de proceder al cese de actividades, ya sea por razones de índole económica, empresaria o de seguridad. También podrá ser motivado por la cancelación de la licencia, dispuesta por la AA o por disolución de la sociedad.

CODE100 S.A., a fin de contemplar esta situación elaboró el documento "Plan de Cese de Actividades", con las estrategias y procedimientos a seguir desde la declaración del cese de actividades hasta la inhabilitación lógica y física de la CA.

Ante la declaración del cese de los servicios de certificación, CODE100 S.A. procederá a la publicación de dicha circunstancia a través del sitio web:

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

- Publicar en su sitio principal de internet la fecha de suspensión de sus servicios con 60 días de anticipación.

- 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.
- Notificar a sus suscriptores por lo menos 30 días antes de la suspensión efectiva o cese de sus operaciones.
- Proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

En caso que el CODE100 S.A., deje de operar, no puede bajo ningún sentido emitir ningún certificado pero debe 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 CODE100 S.A.

El suscriptor, puede 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 puede confiar en dicho certificado.

La DGFD&CE custodiará toda la información referida al cese de operación del PSC, además publicará el cese de actividades o finalización del servicio del PSC en su sitio principal de internet.

6. CONTROLES TÉCNICOS DE SEGURIDAD

Todos los controles serán aprobados por la DGFD&CE, antes de que se pongan en práctica.

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

6.1 Generación e instalación del par de claves

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

6.1.1 Generación del par de claves

El proceso de generación de claves ejecutado por la CA previene la pérdida, divulgación, modificación o acceso no autorizado a las claves privadas que son generadas. Este requerimiento aplica para toda la jerarquía de PKI Paraguay.

Certificados de CODE100 S.A.

La clave privada de la CA es generada en ambientes seguros, por personal autorizado, sobre dispositivos criptográficos homologados FIPS 140-2 Nivel 3. El proveedor de servicios de certificación garantizará que la clave privada de firma nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de claves.

La CA genera sus claves mediante el algoritmo RSA con un tamaño de 4096 bits.

La clave privada de las RA es generada y almacenada por sus responsables, utilizando un dispositivo criptográfico homologado por CODE100 S.A.

Las RA generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

En el caso de los solicitantes y suscriptores, las claves son generadas y almacenadas por ellos mismos mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

Certificados de persona física para firma digital y para autenticación

Las personas físicas podrán hacerlo por "hardware" en un dispositivo criptográfico que deberá ser provisto por el suscriptor y debe estar dentro de los modelos especificados en la lista de los dispositivos homologados por CODE100 S.A.

Certificados de persona jurídica para firma digital y para autenticación

Las personas jurídicas podrán hacerlo por "hardware" en un dispositivo provisto por el suscriptor y debe estar dentro de los modelos especificados en la lista de los dispositivos homologados por CODE100 S.A.

6.1.2 Entrega de la clave privada al suscriptor

Las claves privadas de los suscriptores son generadas por ellos mismos por hardware dentro del proceso de solicitud del certificado, absteniéndose CODE100 de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de la firma.

6.1.3 Entrega de la Clave Pública al emisor del Certificado

El Solicitante entrega la clave pública a la CA durante el proceso de Solicitud de Certificado.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión", remitiendo los datos del Solicitante y su clave pública dentro de una estructura firmada con su clave privada.

El Solicitante debe probar su identidad y demostrar que la solicitud le pertenece, presentando la Solicitud en la cual se identifica el resumen criptográfico.

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

La distribución de la clave pública se realiza a través del certificado digital y del repositorio público respectivo.

6.1.5 Tamaño de la clave

El tamaño de las claves debe ser suficientemente largo para prevenir que otros puedan determinar la clave privada utilizando cripto-análisis durante el periodo de uso del par de claves.

Certificado de CA

El tamaño de las claves para las CA debe tener mínimo 4096 bits RSA.

Certificado de persona física y jurídica

El tamaño de las claves para el suscriptor debe ser de 2048 bits RSA. La longitud de la clave pública que será certificada por la CA, debe ser menor o igual al tamaño de la clave privada de firma de la CA.

6.1.6 Generación de parámetros de clave pública y verificación de calidad

No se establecen condiciones especiales para la generación de parámetros de claves asimétricas más allá de los que corresponden con el algoritmo de generación RSA según su especificación técnica.

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

Certificado de PSC

La Clave privada del PSC podrá ser utilizado con el único propósito de:

- Firmar los certificados de sus Suscriptores; y,
- Firmar la CRL correspondiente

El valor del campo key usage para este certificado es: KeyCertsign=1; CRLSign=1.

Certificado de persona física para firma digital

El valor del campo key usage para este certificado es: nonRepudiaton=1.

Certificado de persona física para autenticación

El valor del campo key usage para este certificado es: digitalSignature=1; KeyEncipherment=1.

Certificado de persona jurídica para firma digital

El valor del campo key usage para este certificado es: NonRepudiaton=1.

Certificado de persona jurídica para autenticación

El valor del campo key usage para este certificado es: DigitalSignature=1; KeyAgreement=1; KeyEnchipherment=1.

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

6.2.1 Estándares y controles del Módulo criptográfico

Certificado de CA

La clave privada de la CA es generada y almacenada sobre un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 3.

Certificado de persona física para firma digital y autenticación

La clave privada del suscriptor persona física es generada y almacenada por "hardware" sobre dispositivos criptográficos de propiedad del suscriptor que cumplen con las normas FIPS 140-2 nivel 2 . El modelo del dispositivo debe ser alguno de los especificados en la lista de dispositivos homologados por CODE100 S.A.

Certificado de persona jurídica para firma digital y para autenticación

La clave privada del suscriptor persona jurídica es generada y almacenada por "hardware" sobre dispositivos criptográficos de propiedad del suscriptor que cumplen con las normas FIPS 140-2 nivel 3 . El modelo del dispositivo debe ser alguno de los especificados en la lista de dispositivos homologados por CODE100 S.A.

6.2.2 Control multi-persona de clave privada

Certificado de CA

La clave privada de la CA es activada exclusivamente en las instalaciones de CODE100 S.A. o en su sitio alternativo de contingencia, dentro del nivel de seguridad asignado a las operaciones críticas de la CA. Para su activación deben estar presentes, personal autorizado en un número M (3), de N (10) posibles.

Certificado de persona física para firma digital y para autenticación

Sin estipulaciones.

Certificado de persona jurídica para firma digital y para autenticación

Sin estipulaciones.

6.2.3 Custodia de la clave privada

La CA no podrá almacenar ni copiar las claves privadas de sus suscriptores. En caso de compromiso de su clave privada estos suscriptores deberán proceder a la revocación de su certificado.

6.2.4 Respaldo de la clave privada

Copias de la clave privada de la CA son realizadas inmediatamente después de su generación, por personal autorizado de CODE100 S.A. y almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3. Estos dispositivos son resguardados en un lugar de acceso restringido.

No se implementa mecanismos de copias de resguardo de la clave privada de las RA ni de los suscriptores.

6.2.5 Archivado de la clave privada

Las copias de resguardo de la clave privada de la CA son conservadas en lugares seguros, al igual que sus elementos de activación, bajo los niveles de seguridad exigidos por la normativa vigente.

No se implementan mecanismos de archivo de copias de resguardo de la clave privada de las RA ni de los suscriptores.

6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico

Las copias de resguardo de la clave privada de la CA están soportadas en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

Las claves privadas de los suscriptores son generadas y almacenadas en dispositivos criptográficos homologados FIPS 140-2 nivel 2 y no permiten su exportación.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

La clave privada de la CA es almacenada y utilizada dentro de un dispositivo criptográfico de hardware seguro que cumple con el estándar FIPS 140-2 nivel 3.

Los dispositivos criptográficos utilizados para el almacenamiento del respaldo de la clave privada de la CA son resguardados de forma segura, en un sitio alterno, con los mismos niveles de seguridad que el sitio principal, para que sea recuperado en el caso de un desastre.

Las RA y los suscriptores de certificados que usen dispositivos criptográficos tienen acceso a su clave privada personal a través de una contraseña de acceso al dispositivo criptográfico y la contraseña de la clave privada.

6.2.8 Método de activación de clave privada

Certificado de CA

Para la activación de la clave privada de la CA se aplica el control M de N. Todos los responsables necesarios para la activación deberán identificarse frente al sistema según corresponda al rol asignado y en un orden determinado por medio de distintos mecanismos de autenticación, a saber: llave de seguridad, claves secretas o ambos.

Las RA tienen acceso a su clave privada personal a través de una contraseña de acceso al dispositivo criptográfico y la contraseña de la clave privada.

Certificado de persona física para firma digital y para autenticación

Los métodos de activación de claves para un usuario deben contar con al menos un factor de seguridad.

Certificados de persona jurídica para firma digital y para autenticación

Los métodos de activación de claves para un usuario deben contar con al menos un factor de seguridad.

6.2.9 Métodos de desactivación de la clave privada

Certificado de CA

La desactivación de la clave privada de la CA puede realizarse en esta implementación, desactivando la partición que la contiene. Esta tarea requiere seguir un procedimiento de excepción.

Cuando la clave privada de la CA fuera desactivada, por expiración o revocación, ésta debe ser eliminada del módulo criptográfico. Se debe asegurar que no se permita la recuperación de copias.

Certificado de persona física para firma digital y para autenticación

Sin estipulaciones.

Certificado de persona jurídica para firma digital y para autenticación

Sin estipulaciones.

6.2.10 Destrucción de clave privada

El procedimiento para la destrucción de las claves privadas debe incluir la autorización para destruirlas.

Certificado de CA

Una vez finalizada la vida útil de la clave privada de la CA, la partición del dispositivo criptográfico contenedor de esa clave privada será borrada e inicializada a cero.

Esta tarea se realizará en el Sitio de Máxima Seguridad en una Ceremonia preparada a ese efecto, con personal autorizado y con los procedimientos de seguridad establecidos.

Certificado de persona física para firma digital y para autenticación

Para el caso de que finalice la vida útil de la clave privada de un suscriptor, por motivo de revocación o expiración del certificado asociado, y sin mediar renovación, deberá ser eliminado el certificado asociado al par de claves correspondiente.

Certificado de persona jurídica para firma digital y para autenticación

Para el caso de que finalice la vida útil de la clave privada de un suscriptor, por motivo de revocación o expiración del certificado asociado, y sin mediar renovación, deberá ser eliminado el certificado asociado al par de claves correspondiente.

6.2.11 Clasificación del Módulo criptográfico

La capacidad del módulo criptográfico de CODE100 S.A. cumple con el estándar Fips 140-2, nivel 3.

Los dispositivos criptográficos de los usuarios personas físicas cumplen con el estándar Fips 140-2, nivel 2.

Los dispositivos criptográficos de los usuarios personas jurídicas cumplen con el estándar Fips 140-2, nivel 3.

6.3 Otros aspectos de gestión del par de claves

La CA debe establecer los medios necesarios para gestionar en forma segura las claves de los suscriptores durante el ciclo de vida de las mismas.

6.3.1 Archivo de la clave pública

Los certificados emitidos a Suscriptores y a las RA, como así también el de la CA, son almacenados y publicados bajo un esquema de redundancia y respaldados en forma periódica, esto, sumado a la firma de cada uno de ellos, garantiza su integridad.

Todos los certificados son almacenados en soporte magnético, en formato estándar bajo codificación internacional DER. No se requieren herramientas particulares para el tratamiento de dicha información.

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

Los periodos de uso de la clave son descriptos en la sección "5.6 Cambio de clave" de la presente CP.

6.4 Datos de activación

La CA mantiene estrictos controles en los datos de activación para operar los módulos criptográficos y que necesitan ser protegidos. (ejemplo un PIN, un código de acceso o "password", autenticación biométrica).

6.4.1 Generación e instalación de los datos de activación

La generación e instalación de los datos de activación de la clave privada de la CA se realiza durante la Ceremonia Inicial con la participación de los N posibles testigos del control M de N.

Como paso previo a la generación de la clave privada, las RA y los suscriptores deberán establecer una clave de seguridad de acceso sobre el dispositivo criptográfico denominado contraseña y al momento de la generación, la contraseña de la clave privada. La contraseña de acceso del dispositivo criptográfico y la contraseña de la clave privada, son conocidas sólo por su titular, ya sea una RA o un suscriptor, con el propósito de proteger la clave privada e impedir el acceso por parte de terceros, incluida la CA.

6.4.2 Protección de los datos de activación

Las RA y los Suscriptores son responsables de la custodia de sus respectivos dispositivos criptográficos y de la no divulgación de la contraseña de acceso del dispositivo criptográfico ni de la contraseña de la clave privada.

Ni CODE100 S.A., ni las RA implementan mecanismos de respaldo de las contraseñas de la clave privada ni de la contraseña de acceso del dispositivo criptográfico de RA ni de Suscriptores.

Los datos de activación de la clave privada de la CA están protegidos por mecanismos de seguridad implementados en el nivel 6 del Sitio de Máxima Seguridad.

6.4.3 Otros aspectos de los datos de activación

Es responsabilidad de las RA y de los Suscriptores, elegir contraseñas para sus claves privadas y contraseñas de acceso del dispositivo criptográfico que:

- Contengan como mínimo 8 símbolos, que incluyan letras mayúsculas, letras minúsculas y números; y
- No sean fácilmente deducibles por otros, evitando utilizar nombres, direcciones, números telefónicos y similares relacionados con el Suscriptor.
- Establecer una frecuencia de actualización de los datos de activación. Los datos de activación de los módulos criptográficos del PSC deben ser cambiados al menos una vez cada seis meses. Para los suscriptores se recomienda cambiar los datos de activación periódicamente.
- La contraseña de acceso del dispositivo criptográfico debe diferir de la contraseña de la clave privada.

6.5 Controles de seguridad del computador

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Para la prestación de sus servicios, la CA utiliza una infraestructura tecnológica propia que cumple con los requisitos técnicos establecidos por la normativa vigente.

Entre los controles técnicos utilizados pueden mencionarse:

- **Control de Acceso físicos y lógicos**

  El acceso físico a las instalaciones está conformado por diversos perímetros de seguridad internos unos de otros, cada uno de los cuales cuenta con mecanismos de tarjeta de proximidad y/o biométricos. Del mismo modo, el acceso lógico a los sistemas se realiza por medio de servidores "firewall" y sus propios mecanismos de control y monitoreo. Los equipos donde operan los sistemas de la CA en caso de contar con acceso remoto, se implementan con autenticación mutua.

- **Separación de funciones y roles críticos**

  Las principales funciones vinculadas a los procesos de certificación se encuentran divididos en roles que aseguran el correcto desempeño de los responsables designados. Los roles definidos en la operatoria de la CA serán desempeñados por los responsables designados. En caso de ausencia temporaria, el responsable será reemplazado por el correspondiente sustituto designado.

- **Identificación y autenticación de roles**

  Para la identificación y autenticación en cada uno de los roles críticos vinculados al proceso de certificación y gestión de claves de CODE100 S.A., se utilizan mecanismos de reconocimiento biométrico y sistemas de autenticación de múltiples factores.

- **Utilización de criptografía para las sesiones de comunicación**

  Todas las comunicaciones críticas entre los distintos componentes de la CA se realizan en forma cifrada.

- **Archivo de datos históricos y de auditoría del PSC y usuarios**

  Se realizan auditorías y controles periódicos sobre cada etapa del proceso de certificación, incluyendo la verificación de la documentación de respaldo del proceso de identificación de suscriptores.

- **Registro de eventos de seguridad**

Todas las operaciones y actividades de CODE100 S.A. generan información de control y registros de eventos que permiten verificar el funcionamiento y la seguridad de los sistemas.

- **Prueba de seguridad**

  Se realizan comprobaciones periódicas del funcionamiento de los sistemas y los planes de contingencia.

- **Mecanismos confiables para identificación de roles afectados al proceso de certificación**

  Existen mecanismos confiables de identificación de roles, en forma redundante, para los que intervienen en el proceso de certificación.

- **Mecanismos de recuperación para claves y sistema de certificación**

  Existen mecanismos y procedimientos de contingencia que garantizan la continuidad en la prestación de los servicios.

6.5.2 Clasificación de la seguridad del computador

Los servidores que conforman la CA se encuentran alojados en el "Sitio de Máxima Seguridad" o SMS construido con los estándares requeridos para este tipo de ambientes.

Las certificaciones del módulo criptográfico HSM son las siguientes:

- U/L 1950 & CSA C22.2 y en CSA C22.2
- FCC Part 15 – Clase B
- High Assurance HSM
- Common criteria EAL 4+
- FIPS 140-2 Nivel 3

Aplicación PKI CA CODE100:

El software PKI utilizado por la CA se basa en los servicios de certificados nativos del producto Microsoft Windows Server, permitiendo a su vez darle soporte documental a todos los circuitos diseñados para implementar la infraestructura de clave pública. Es un software totalmente escalable, modular e integrable, e incluye todas las llamadas a las funciones de Microsoft Windows Server que cuenta con un completo sistema de seguridad diseñado según las normativas de seguridad ITU: X.509v3, RSA: PKCS 1, 7, 9, 10, 12 y IETF: RFC5280 upd by 6818, CMC.

6.6 Controles técnicos del ciclo de vida

La CA mantiene controles en los equipos de seguridad (hardware y software) requeridos para operar en una infraestructura PKI desde el momento de la compra hasta su instalación, de forma que reduzcan la probabilidad que cualquiera de sus componentes sea violentado.

Todo el hardware y software que ha sido identificado para operar las CA es enviado y entregado con métodos que provean una adecuada cadena de custodia. Y además, las configuraciones son verificadas en un ambiente de prueba antes de iniciar operaciones.

6.6.1 Controles para el desarrollo del sistema

La CA mantiene controles que proporcionen una seguridad razonable de las actividades de desarrollo y mantenimiento de los sistemas de la CA.

Los nuevos sistemas o para la expansión de los sistemas existentes, especifican los requisitos de control, siguen procedimientos de prueba de software y control de cambios para la implementación de software. Toda la documentación del ciclo de vida del sistema, debe estar disponible para su verificación.

La CA mantiene controles sobre el acceso a las bibliotecas fuente de programas.

Los sistemas informáticos son homologados por personal técnico al momento de su implementación, para asegurar que los programas que se ponen en producción respondan a las características de diseño declaradas por el proveedor y oportunamente aceptadas cuando fueron seleccionados.

6.6.2 Controles de gestión de seguridad

Los Administradores de la CA son los responsables de garantizar que se cumplan los procedimientos de seguridad correctamente. Además de ejecutar revisiones periódicas para asegurar el cumplimiento de los estándares de implementación de seguridad.

La CODE100 S.A. mantiene el control de los equipos y de la documentación de la configuración del sistema, registrándose toda modificación o actualización a cualquiera de ellos.

El esquema de seguridad física del SMS de la CA previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones.

6.6.3 Controles de seguridad del ciclo de vida

La CA realiza controles en la gestión de seguridad por medio de herramientas y procedimientos que verifican la adherencia a la configuración de seguridad de los sistemas operativos y redes.

6.7 Controles de seguridad de red

El equipo de la CA se encuentra dentro de los límites de la red interna, operando bajo un nivel de seguridad de red crítico. La red de la CA está protegida contra ataques. Los puertos y servicios que no se requieran se encuentran apagados. Los sitios Web del PSC están provistos de certificados SSL.

CODE100 S.A. posee un sistema de protección integral de sus activos informáticos. La red de la CA, está aislada de otras redes y se encuentra delimitada por diversos cortafuegos ("firewalls") que proveen el filtrado de los paquetes de datos.

6.8 Sellado de tiempo (Time-stamping)

No aplica.

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

Todos los certificados emitidos bajo la presente CP respetan la especificación ITU-T X.509 (ISO/IEC 9594-8) "Information Technology – The Directory: Public key and atribute certificate frameworks".

7.1 Perfil del Certificado

El certificado digital debe cumplir con:

- 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" Cómo mínimo el certificado contiene:

Campo	**Valor o restricciones**
Versión (Version)	Los certificados deben ser X.509 versión 3 (V3).
Número de serie (Serial number)	Valor único emitido dentro del ámbito de cada CA.
Algoritmo de firma (Signature algorithm)	El Algoritmo de firma debe ser como mínimo SHA 256 RSA.
Emisor (Issuer DN)	Nombre de la CA Ver sección "7.1.4 Formas de Nombre"
Válido desde (Valid from)	Este Campo especifica la fecha y hora a partir de la cual el certificado es válido. Las fechas establecidas para el periodo de validez deben ser sincronizadas con respecto a la hora oficial de la República del Paraguay.
Válido hasta (Valid to)	Este Campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Las fechas para la validez del certificado deben ser sincronizadas con el horario oficial de la República del Paraguay.
Sujeto (Suscriber DN)	Nombre del suscriptor. Ver sección "7.1.4 Formas de Nombre"
Clave pública del sujeto (Subject Public Key)	Codificado de acuerdo con el RFC 5280. Con un largo de clave mínima de 2048 bits y algoritmo RSA.
Extensiones	
Identificador de la clave del titular (Subject Key Identifier)	Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.
Identificador de la Clave Publica del Emisor (Authority Key Identifier)	La extensión de identificador de clave autoridad emisora proporciona un medio del la identificación de la clave pública correspondiente a la clave privada utilizada

	para firmar un certificado.
Política del certificado (Certificate Policies)	Describe las políticas aplicables al certificado y la dirección URL donde se encuentra disponible la CP respectiva.
Uso de la clave (Key usage)	Debe indicar los usos permitidos de la clave. Este campo debe ser marcado como un CAMPO CRÍTICO. Ver sección "1.4.1 Usos apropiados del certificado".
Punto de distribución del CRL (Distribuition Points)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.
Acceso a la información de la autoridad (Authority Information Access)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.
Usos extendidos de la clave	Referencia otros propósitos de la clave, adicionales al uso. De acuerdo con la sección "7.1.2.5 Uso extendido de Clave" Solamente en el caso de certificado de persona física o jurídica este campo debe especificarse.
Restricciones básicas (Basic Contraitns)	Ver sección "7.1.2.4 Restricciones básicas"
Huella Digital (Thumbprint)	Resultado de aplicar algoritmos matemáticos a la información.
QcStatements	Conforme al ETSI- TS 101 862 V.1.3.3.

7.1.1 Número (s) de versión

Todos los certificados emitidos dentro de la PKI Paraguay deben corresponder al estándar X.509 versión 3.

7.1.2 Extensiones del certificado

7.1.2.1 Key Usage

El "key usage" indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Ver sección "1.4.1 Usos apropiados del certificado". Es una extensión crítica.

7.1.2.2 Extensión de política de certificados

En la extensión de "certificatepolicies" (Directivas del Certificado) detalla el nombre del dominio elegido por la CA y el directorio creado para el repositorio de dicho documentos. Es una extensión crítica.

7.1.2.3 Nombre alternativo del sujeto

La extensión "subjectAltName" es opcional y solamente se puede usar para certificados de agente de persona jurídica para autenticación. En caso de ser utilizada, el uso de esta extensión es "no crítico" y únicamente está permitido el uso del nombre DNS, en concordancia con la sección "4.1.2. Proceso de inscripción y responsabilidades"

7.1.2.4 Restricciones básicas

Debe tener el valor ''cero", para indicar que el mismo no permite más sub-niveles en la ruta del certificado y en el caso del certificado de persona física o jurídica, este campo no debe especificarse. Es una extensión crítica.

7.1.2.5 Uso extendido de la clave

La extensión permite configurar los propósitos de la clave. La extensión no es crítica.

7.1.2.6 Puntos de distribución de los CRL

La extensión "CRL Distribution Points" (Puntos de Distribución) contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. La extensión no es crítica.

7.1.2.7 Identificador de clave de Autoridad

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

7.1.2.8 Identificador de la clave del sujeto

El método para la generación del identificador de clave está basado en la clave pública del sujeto del certificado y es calculado de acuerdo con uno de los métodos descritos en el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". La extensión no es crítica.

7.1.2.9 QcStatements

El "QcStatements" debe ser definido acorde al estándar ETSI-TS 101 862 V.1.3.3 "Qualified Certificate Profile". La extensión no es crítica.

7.1.3 Identificadores de objeto de algoritmos

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

Identificador de objeto (OID) de algoritmo criptográfico

- sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Identificador de objeto (OID) de clave pública

- RSAEncryption (1.2.840.113549.1.1.1)

7.1.4 Formas del nombre

Los nombres dentro de la PKI Paraguay cumple las regulaciones de la sección "3.1.1 Tipos de nombre".

Adicionalmente, en el campo Suscriber DN (Sujeto) el certificado de suscriptor generalmente incluye el URL donde se encuentra los términos del uso de los certificados y los acuerdos entre las partes.

7.1.5 Restricciones del nombre

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".

7.1.6 Identificador de objeto de Política de Certificado

La DGFD&CE gestiona la obtención del OID correspondiente a cada clase de certificado.

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

Sin estipulaciones.

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

El calificador de la política está incluido en la extensión de "certificate policies" y contiene una referencia al URL con la CP aplicable y a los acuerdos de partes que confían.

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

Sin estipulaciones.

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 (Signature Algorithm)	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 (Certificate Revoked)	Lista de certificados revocados, incluyendo el número de serie del certificado revocado y la fecha de revocación.
Extensiones	
Número CR(CRL Number)	Orden secuencial de emisión de CRL
Identificador de clave de Autoridad(Authority Key Identifier)	Identificador de la clave pública de CA.
Punto de distribución del CRL (Distribuition Points)	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

La PKI Paraguay soporta las CRLs X.509 versión 2.

7.2.2 CRL y extensiones de entradas de CRL

7.2.2.1 Número CRL (CRL Number)

Orden secuencial de emisión de CRL. Esta extensión es 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 delcertificado, de acuerdo a lo descrito por el RFC 5280 "Internet X.509 Public KeyInfraestructura Certificate and CRL Profile". La extensión no es crítica.

7.2.2.3 Puntos de distribución de las CRL

La extensión "CRL Distribution Points"(Puntos de Distribución) contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. 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 se implemente debe cumplir lo estipulado en el RFC-2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.1 Número (s) de versión

Debe cumplir al menos 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

De acuerdo la Ley Nro. 4017/10, Nro. 4610/12, Decreto Reglamentario Nro. 7369/11 se establece que los PSC, deben ser auditados periódicamente, de acuerdo con el sistema de auditoría que diseñe y apruebe el MIC.

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

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

La DGFD&CE o terceros designados por ella es responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la normativa vigente.

El PSC CODE100 implementa un programa de auditorías internas para la verificación de su sistema de gestión.

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

8.1 Frecuencia o circunstancias de evaluación

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

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

8.2 Identidad/calidades del evaluador

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

8.3 Relación del evaluador con la entidad evaluada

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

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

8.4 Aspectos cubiertos por la evaluación

Los elementos objeto de Auditoría son:

- Controles de seguridad física y estándares técnicos de seguridad.
- Confidencialidad y calidad de los sistemas de control.
- Integridad y disponibilidad de los datos.
- Cumplimiento de los estándares tecnológicos.
- Seguridad del Personal.
- Cumplimiento de la Política y Declaración de Prácticas de Certificación.
- Cumplimiento de la legislación vigente, entre otros.

8.5 Acciones tomadas como resultado de una deficiencia

CODE100 tiene procedimientos para ejecutar acciones correctivas para las deficiencias detectadas tanto en las Auditorías externas como en las internas.

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

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

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

8.6 Comunicación de resultados

CODE100 publicará en el sitio principal de internet los informes de las auditorías realizadas.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

Este punto contiene las disposiciones aplicables acerca de los montos a ser percibidos por la CA.

9.1.1 Tarifas de emisión y administración de certificados

La tarifa por la emisión y administración de los certificados emitidos por una CA, estará determinada en la normativa vigente.

Los certificados digitales emitidos bajo la presente CP 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/medio de pago.html

9.1.2 Tarifas de acceso a certificados

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

9.1.3 Tarifas de acceso a información del estado o revocación

El acceso a la información de estado o revocación a través de consulta de la CRL disponible en el sitio de internet es gratuito. CODE100 S.A. puede cobrar una tarifa por servicio de OCSP u otros servicios de valor agregado sobre servicios de estado y revocación, cuyos costos se publicaran en el sitio de internet.

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

9.1.4 Tarifas por otros servicios

La CA, no se encuentra habilitada para el cobro de tarifas para acceder a información de la CP y la CPS.

9.1.5 Políticas de reembolso

La Política de Reembolsos del PSC CODE100 S.A. comprende los Certificados Digitales que emite bajo su Políticas de Certificación.
Ante las siguientes circunstancias:

- El solicitante presenta un reclamo sobre un certificado digital emitido por 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.
- 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

CODE100 S.A. será responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de esta CP, por los errores u omisiones que presenten los certificados digitales que expide, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá a CODE100 S.A. demostrar que actuó con la debida diligencia.

9.2.1 Cobertura de seguro

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

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

En el caso que exista cobertura de seguro o garantía disponible para los suscriptores, CODE100 S.A. establece en su CPS los tipos correspondientes.

9.3 Confidencialidad de la información comercial

Como principio general, se establece que toda información remitida por el solicitante de un certificado al momento de efectuar un requerimiento debe ser considerada confidencial y no ser divulgada a terceros sin el consentimiento previo del solicitante o suscriptor, salvo que sea requerida por juez competente o bien como parte de un proceso judicial o administrativo. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso al CA durante el ciclo de vida del certificado.

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 CODE100 S.A. como sus RA no podrán divulgar los datos de los suscriptores sin su consentimiento. Asimismo, 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, no confidencial y accesible por terceros a:

a) CP de CODE100
b) CPS de CODE100.
c) Certificado de la CA Raíz de Paraguay.
d) Certificado de la CA CODE100.
e) Lista de Certificados Revocados.
f) Acuerdo con Suscriptores.
g) Las Resoluciones que Habilitan, Suspenden o Revocan al PSC.
h) La información relevante de la última auditoría que hubiere sido objeto.
i) Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay.
j) Identificación, domicilio y medios de contacto.

9.4 Privacidad de información personal

9.4.1 Plan de Privacidad

La CA 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.

9.4.4 Responsabilidad para proteger información privada

La CA asegura que la información privada no sea comprometida o divulgada a terceras partes.

9.4.5 Notificación y consentimiento para usar información privada

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

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 aplicable.

9.5 Derecho de Propiedad intelectual

CODE100 S.A. es propietaria exclusiva de todos los derechos de propiedad intelectual de la presente CP, acuerdos, declaraciones, procedimientos y documentos auxiliares referidos a la CA, así como la documentación y contenidos del sitio web de la CA que se encuentra en:

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

Asimismo, es titular del derecho de propiedad intelectual de las aplicaciones informáticas propias, excepto los sistemas operativos de soporte informáticos no desarrollados por CODE100 S.A. que cuentan con sus respectivas licencias de uso.

CODE100 S.A. es única y exclusiva propietaria de la presente CP, y sus documentos relacionados reservándose todos los derechos de autor establecidos en la legislación vigente de derechos de propiedad intelectual.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

La CA debe garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión de los mismos.
- No existan errores en la información que fue introducida por la entidad que aprueba la emisión del certificado.
- Los certificados reúnen los requerimientos expuestos en esta CP.
- Los servicios de revocación y el uso de los repositorios cumplen lo estipulado en esta CP.

9.6.2 Representaciones y garantías de la RA

El PSC en su función de RA asegura que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No se presentan errores en la información del certificado que fue introducida por las entidades de registro.
- Que los dispositivos y materiales requeridos cumplen con lo dispuesto en esta CP.

9.6.3 Representaciones y garantías del suscriptor

El suscriptor garantiza que:

- Cada firma digital creada usando la clave privada corresponde a la clave pública listada en el certificado.
- La clave privada está protegida y que no autoriza a otras personas a tener acceso a la clave privada del suscriptor.
- Toda la información facilitada por el suscriptor y contenida en el certificado es verdadera.
- El certificado es utilizado exclusivamente para los propósitos autorizados.

9.6.4 Representaciones y garantías de las partes que confían

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

9.6.5 Representaciones y garantías de otros participantes

Sin estipulaciones.

9.7 Exención de garantía

La CA establece en su CP, CPS y otra documentación relevante, cualquier exención de responsabilidad que pudiera aplicárseles.

9.8 Limitaciones de responsabilidad legal

La CA establece en su CP, CPS u otra documentación relevante cualquier limitación de responsabilidad que pudiera aplicársele, considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación establecidas en este documento.

9.8.1 Limitaciones del responsabilidad del PSC

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

9.9 Indemnizaciones

El PSC 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.

9.10 Plazo y finalización

9.10.1 Plazo

La CP 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.

9.10.2 Finalización

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

9.10.3 Efectos de la finalización y supervivencia

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

9.11 Notificación individual y comunicaciones con participantes

Toda comunicación entre la CA y el suscriptor, se realizará mediante mensaje de datos firmado digitalmente o documento escrito dirigido a cualquiera de las direcciones establecidas como contacto. Las comunicaciones electrónicas se harán efectivas una vez que la reciba el destinatario al que van dirigidas de igual manera en el caso de las escritas.

9.12 Enmiendas

9.12.1 Procedimientos para enmiendas

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

Los cambios efectuados en la CP y CPS de los PSC deben ser revisados y aprobados por la DGFD&CE, 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 CP, se publicará en el sitio principal de internet de la CA.

9.12.3 Circunstancias en que los OID deben ser cambiados

Sin estipulaciones.

9.13 Disposiciones para resolución de disputas

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

9.14 Normativa aplicable

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

9.15 Adecuación a la ley aplicable

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

9.16 Disposiciones varias

9.16.1 Acuerdo completo

No aplica.

9.16.2 Asignación

No aplica.

9.16.3 Divisibilidad

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

9.16.4 Aplicación (Honorarios de Abogados y renuncia de derechos)

No aplica.

9.16.5 Fuerza mayor

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

9.17 Otras disposiciones

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

Esta CP y CPS guarda concordancia con las disposiciones de la Infraestructura de Clave Pública del Paraguay.

10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP".
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- ISO 3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- Ley Nro. 4017/2010 '"De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico"
- Ley Nro. 4610/2012 que modifica y amplía la Ley Nro. 4017/2010

- Decreto Reglamentario Nro. 7369/2011
- CP de la Infraestructura de Clave Pública de Paraguay.