MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN (PÚBLICO)

VERSIÓN 1.6.2 – FECHA 10/10/2019

CLASE: Público

Firmado digitalmente por:
ACOSTA CASTILLO FABIAN ARISTIDES
Fecha: 13/12/2019 07:57:40

VERSIONES Y MODIFICACIONES DE ESTE DOCUMENTO

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	2014-04-04	GrupoFD	Directorio	Aprobación para presentación
1	1	2014-12-22	GrupoFD	Directorio	Aprobación para presentación
1	2	2014-12-29	GrupoFD	Directorio	Aprobación para presentación
1	3	2014-12-29	GrupoFD	Directorio	Aprobación para presentación
1	4	2014-04-28	GrupoFD	Directorio	Aprobación para presentación
1	5	2017-02-01	GrupoFD	Directorio	Adecuación procedimiento de identificación.
1	6	2017-02-03	GrupoFD	Directorio	Aprobación para presentación
1	6.1	2017-05-10	GrupoFD	Directorio	Revisión y aprobación del documento
1	6.2	2019-10-10	Fabian Acosta	Rocio Vazquez	Revisión y aprobación del documento

INDICE

1. INTRODUCCIÓN

1.1. Contenido del Manual de Procedimientos

El Manual de Procedimientos de Certificación describe las actividades requeridas para la puesta en marcha y prestación del servicio de certificación de CODE100 S.A. como Prestador de Servicios de Certificación (en adelante "PSC") y está estrechamente ligado al documento CP.

Esas actividades constituyen procedimientos específicos, para cada uno de los cuales se indican todos o algunos de los siguientes datos:

- Consideraciones
- Requisitos
- Objetivo
- Frecuencia, oportunidad y urgencia
- Roles que participan en el procedimiento
- Acción que pone en marcha el procedimiento
- Tareas a realizar por cada uno de los roles que actúan
- Resultado del procedimiento

Este Manual está dividido en dos partes, presentadas como dos documentos por separado pero con una estrecha relación, dado que uno es complementario del otro.

1.1.1. Documento Público

El documento de acceso público es para conocimiento de las partes involucradas: PSC con su CA y RA, solicitantes, suscriptores y parte en que confía. También está libremente disponible para todo aquél que esté interesado en la información que él contiene.

El presente es el documento público.

1.1.2. Documento Reservado

El documento reservado es complementario del documento público y contiene la información propia de la administración del servicio, que no se publica por razones de seguridad y confidencialidad.

1.2. Identificación de este Documento

Nombre: Manual de Procedimientos de Certificación (Público)

Versión: 1.6.1

Fecha: 10/05/2017

Lugar: República del Paraguay

1.3. Participantes y aplicabilidad

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. Autoridades de Registros (RA)

Las RA y RA Delegadas que se encuentran habilitadas por el PSC CODE100 S.A. para los procesos de recepción, validación y direccionamiento de solicitudes de emisión o de revocación de certificados digitales, y de identificación de sus solicitantes.

Las Autoridades de Registro habilitadas se publicarán en el sitio:

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

Las RA delegadas son autoridades de registro vinculadas a un PSC mediante un contrato de prestación de servicios; el funcionamiento de las mismas deberá estar en conocimiento y autorizadas por la CA raíz.

1.3.3. Prestadores de Servicios de Soporte (PSS)

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

a) Disponibilización de infraestructura física y lógica;

b) Disponibilización de recursos humanos especializados;

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

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

http://www.code100.com.py/prestadores-servicios-soporte.html

1.3.4. Suscriptores

En relación a CODE100 S.A, es suscriptor toda persona física o jurídica titular de los certificados emitidos según esta CP.

1.3.5. - Parte que confía

Es toda persona física o jurídica diferente al titular del certificado que decide aceptar y confiar en un certificado digital emitido dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.6. – Otros Participantes

Sin estipulaciones.

1.4. Contactos

El Manual de Procedimientos de Certificación es administrado por CODE100 S.A.:

Nombre: Carlos E. M. Dossetti

Dirección: Asunción, Paraguay

Teléfono: (+595) (21) 444789

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

Para realizar preguntas, efectuar reclamos o enviar sugerencias referidos al proceso de certificación el interesado deberá dirigirse a:

Nombre: Carlos E. M. Dossetti

Dirección: Asunción, Paraguay

Teléfono: (+595) (21) 44789

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

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.

Code100 garantiza la vigencia que producida una actualización del marco legal u operativa del PSC, la nueva versión de los documentos relacionados con dicho marco normativo se publicará de acuerdo a lo establecido en el punto 9.12 de la correspondiente CP de CODE100 S.A.

El PSC 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 la

documentación referenciada, pero CODE100 S.A. establece controles de seguridad para prevenir que personas no autorizadas agreguen o modifiquen información de los repositorios.

- **Frecuencia, oportunidad y urgencia**

Dentro de las 24 hs. la notificación de un cambio o de la actualización y aprobación de una nueva versión de un documento.

- **Roles que participan en el procedimiento**

a) Jefe de Área

b) Administrador de Sistemas

- **Acción que pone en marcha el procedimiento**

Tomar conocimiento de la actualización de un documento cuya publicación es requerida por la normativa vigente.

- **Tareas a realizar por cada uno de los roles que actúan**

a) El Administrador de Sistemas realiza la publicación en el repositorio público del documento actualizado.

b) El Jefe de Área verifica que el documento esté actualizado y disponible en el repositorio.

- **Resultado del procedimiento**

  - Documento actualizado publicado en repositorio público.

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 de Certificación", se publicará de acuerdo a lo establecido en el punto "9.12 Enmiendas" de la 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 Frecuencia de Emisión del CRL" de la CP.

2.4 Controles de Acceso

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.

2.5. - Publicación y repositorios de Certificados y Listas de Certificados Revocados (CRLs)

La publicación se hará de acuerdo con lo indicado en "2.2 Pubicación de Información de Certificación" y "2.3 Tiempo y frecuencia de Publicación" de la CP.

La publicación de información de la CA se realiza en sus servidores, y se puede encontrar en el sitio web identificado como:

http://www.CODE100.com.py/firma-digital

El detalle de los procedimientos para la publicación es información reservada que se encuentra en el manual de procedimientos reservado.

2.6. Auditorías

La AA de la Infraestructura de Firma Digital del Paraguay realiza auditorías ordinarias a la CA y a sus RA, a fin de verificar el cumplimiento de los requisitos para la habilitación.

Esas auditorías tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener la condición de PSC y la aplicación de las políticas y procedimientos aprobados por la AA para la CP.

Los temas principales a evaluar en dichas auditorías son:

a) Requisitos legales generales.

b) CP y Manual de Procedimientos de Certificación.

c) Plan de Seguridad.

d) Plan de Cese de Actividades.

e) Plan de Contingencia, Recuperación frente a desastres y Continuidad del negocio.

f) Plataforma Tecnológica.

g) Ciclo de vida de las claves criptográficas del certificador.

h) Ciclo de vida de los certificados de suscriptores.

i) Estructura y contenido de los certificados y CRLs.

j) Mecanismos de acceso a la documentación publicada, certificados y CRLs.

k) Pautas para la RA.

Por su parte, CODE100 S.A. realizará con su Administrador de Auditoría, auditorías periódicas a sus RA habilitadas, para verificar el cumplimiento de los requisitos de su habilitación, siendo los temas principales a evaluar:

a) Lo establecido en el documento "Guía de instalación y funcionamiento de las RA"

b) Las políticas y procedimientos aprobados por la AA para la CP de CODE100 S.A.

En caso de producirse observaciones en las auditorías realizadas, luego de haber sido debidamente notificadas a la RA auditada. CODE100 S.A. tomará las medidas correctivas de carácter legal y técnico que amerite el caso. Estas pueden ser desde la supervisión del plan de acción confeccionado por la RA auditada para resolver las no conformidades hasta la aplicación de sanciones a la RA auditada. Los resultados de la auditorías realizadas son presentadas por el Administrador de Auditoría el cual evaluará los informes obtenidos y los elevará al Directorio de CODE100.

2.6.1. Procedimiento de Auditoría Interna a las RA

- **Frecuencia, oportunidad y urgencia**

Se realizara una auditoría con periodicidad anual a partir de la fecha de la última auditoría. Planificada. Sin fecha fija. Urgencia baja, salvo situación excepcional.

- **Roles que participan en el procedimiento**

a) Administrador de Auditoría

b) Responsable de Firma Digital

c) Oficial de Registro

- **Acción que pone en marcha el procedimiento**

Decisión tomada por la RA Central de CODE100 S.A., de realizar una auditoría interna a la RA seleccionada.

Cumplimiento de un año desde la última auditoría.

Tareas a realizar por cada uno de los roles que actúan

d) El Administrador de Auditoría llevará a cabo las visitas necesarias a los roles a auditar.

e) Elaborará un informe de auditoría y lo entregará a los roles auditados, con copia al Responsable de Firma Digital.

f) Los roles auditados corregirán o modificarán lo necesario, de acuerdo a las observaciones del informe de Auditoría Interna.

g) Los roles auditados responderán a Auditoría Interna mediante un informe, Responsable de Firma Digital.

h) El Responsable de Firma Digital evaluará el informe de auditoría y la respuesta de los roles auditados.

i) Se definirá el plan de acción de las no conformidades y luego de su presentación y autorización se ejecutara.

j) En caso de corresponder, el Responsable de Firma Digital aplicará las sanciones necesarias, de acuerdo con lo establecido en el punto 5.3.5. Sanciones a aplicar por acciones no autorizadas"" de este Manual de Procedimientos.

- **Resultado del procedimiento**
  - Informe de Auditoría Interna.
  - Respuesta al Informe por parte de los roles auditados.
  - Plan de acción de no conformidades.
  - En caso de corresponder, sanciones aplicadas.

2.7. – Confidencialidad

Según lo descripto en "9.3. Confidencialidad de la información comercial" de la CP.

2.8. - Derechos de Propiedad Intelectual

CODE100 S.A. es propietaria exclusiva de todos los derechos de propiedad intelectual de la 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.

3. IDENTIFICACION Y AUTENTICACION

3.1. Registro inicial

La descripción del registro inicial está contenida en "3.1 Registro inicial" de la CP. Es importante acceder y tomar conocimiento de ella, particularmente de la información que el solicitante debe consultar y tener presente antes de iniciar su solicitud.

3.1.1. -Tipos de Nombres

No se establecen restricciones a los nombres que pueden ser incluidos dentro de los certificados, en tanto se correspondan con la documentación probatoria exigida para la emisión de certificados por la CP.

3.1.2. - Necesidad de Nombres Distintivos

La necesidad del uso de nombres distintivos está expuesta en "3.1.2. Necesidad de Nombres significativos" de la CP, donde se presenta esta cuestión tanto para personas físicas como para personas jurídicas.

3.1.3. - Reglas para la interpretación de nombres

Rige lo establecido en "3.1.4. Reglas para interpretación de varias formas de Nombres" de la CP, que se transcribe:

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

3.1.4. - Unicidad de los nombres

La CP cumple en lo que respecta a la necesidad de que el nombre distintivo sea único. Si dos o más suscriptores tuvieran el mismo nombre y apellido, o el mismo nombre de persona jurídica, la unicidad queda resuelta por medio de los atributos citados en "3.1. 5. Unicidad de Nombres" de la CP.

3.1.5. - Procedimiento de resolución de disputas sobre nombres

- **Frecuencia, oportunidad y urgencia**

Disponible en forma permanente. No planificado. Urgencia baja.

- **Roles que participan en el procedimiento**

a) Responsable de Firma Digital

b) Oficial de Registro

c) Solicitante

- **Acción que pone en marcha el procedimiento**

Disputa o conflicto en la utilización de nombres para titulares de certificados de persona física o de persona jurídica.

- **Tareas a realizar por cada uno de los roles que actúan**

a) El solicitante presenta su reclamo por nota ante el Oficial de Registro.

b) El Oficial de Registro evalúa y convoca al Responsable de Firma Digital para tratar el reclamo.

c) Los roles intervinientes dirimen la disputa tomando como criterio lo establecido en "3.1.4. Reglas para interpretación de varias formas de Nombres" de la CP.

d) El Responsable de Firma Digital resolverá lo que estime corresponder, conforme a criterios de máxima razonabilidad, equidad y pleno ajuste a la normativa vigente y aplicable en la especie.

e) Se asienta la decisión tomada en el Libro de Actas de la RA.

f) El Oficial de Registro comunica al correo electrónico informado oportunamente por el solicitante la resolución del reclamo.

- **Resultado del procedimiento**

Identificación de los campos a aplicar en el certificado digital, que conformarán el nombre único del titular y correo electrónico de comunicación de resolución al solicitante.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

Rige lo establecido en "3.1.6. Reconocimiento, autenticación y rol de las marcas registradas" de la CP.

3.1.7. Métodos para comprobar la posesión de la clave privada

El método de comprobación está estrechamente ligado con la generación de la solicitud, dado que ambos se generan mediante un único procedimiento. Esto asegura que, si un solicitante generó y presentó una solicitud de certificado digital, él es poseedor de la clave privada.

Para la comprobación de la posesión de la clave privada se utiliza el siguiente procedimiento:

- El Solicitante es partícipe directo y necesario en la generación de su par de claves criptográficas asimétricas, utilizando su propio equipamiento. Las claves criptográficas no quedan almacenadas en los sistemas informáticos de la CA de CODE100 S.A.
- Durante el proceso de solicitud, se requiere que el Solicitante realice la generación de un par de claves criptográficas asimétricas, dicha operación será realizada en el equipo del solicitante y en ningún momento de la generación los sistemas informáticos de CODE100 tienen contacto con la clave privada del solicitante.

- El Solicitante utilizará un dispositivo criptográfico de su propiedad donde las claves son generadas y almacenadas en él.
- Los datos de la Solicitud y el requerimiento con la clave pública del Solicitante, en formato PKCS#10, son enviados a la aplicación del PSC.
- La aplicación del Certificador valida el requerimiento PKCS#10 y verifica automáticamente mediante un algoritmo de control la existencia de la correspondencia de la clave privada asociada a la clave pública incluida en este requerimiento al momento de su generación.
- En caso de ser correcto el formato, la aplicación del PSC entrega al Solicitante una Solicitud completa incluyendo el resumen criptográfico (huella MD5).
- El Solicitante debe imprimir la Solicitud, para entregar en la RA, cuando se presenta en el proceso de identificación, demostrando así la posesión de la clave privada.

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 la identidad de personas jurídicas

Este proceso tiene como requisito previo la elaboración de la solicitud del certificado digital y la creación del par de claves criptográficas, son parte del Ciclo del certificado y se describen en "4.1.2.2 Certificado de Persona Jurídica para firma digital y para autenticación" de la CP.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Planificado. Urgencia alta.

Se realiza solo en horario laboral.

- **Roles que participan en el procedimiento**

a) Solicitante o suscriptor

b) Oficial Identificador

c) Oficial de Registro

- **Acción que pone en marcha el procedimiento**

Solicitud de identificación de una persona jurídica a la RA.

- **Tareas a realizar por cada uno de los roles que actúan**

El Solicitante, en carácter de, representante legal, apoderado o administrador de la persona jurídica del certificado se presenta ante un Oficial Identificador, con la documentación necesaria, según lo especificado en el punto "4.1.2.2 Certificado de Persona Jurídica para firma digital y para autenticación" de la CP.

El Solicitante será atendido por el Oficial Identificador, quien verificará su identidad, la documentación que presenta y el resumen criptográfico vinculado con la Solicitud, así como toda otra información contenida en la Solicitud.

El Oficial Identificador revisará los comprobantes a presentar:

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

Si la identificación ha sido satisfactoria, el Solicitante firma la solicitud impresa y dos ejemplares impresos del "Acuerdo con Suscriptores", quedando uno en poder del Solicitante y el otro en poder de la RA correspondiente. El Oficial Identificador conserva para el armado de la carpeta del suscriptor la documentación presentada como respaldo del proceso de identificación.

Recibida la documentación en la RA, un Oficial de Registro procederá a efectuar el control de la documentación y comprueba que la información suministrada concuerda con los datos oficiales mediante la consulta a las bases de datos oficiales de verificación de identidad. Luego cargará en la aplicación de la RA la confirmación de los documentos recibidos y determinará la aceptación o rechazo de la Solicitud.

En caso de aprobar la Solicitud, el Responsable Oficial de Registro firmará la misma con su certificado habilitado en la aplicación de la RA.

Finalmente, en caso de aprobación, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona jurídica Solicitante. Esta contiene la Solicitud de Certificado y todos los documentos presentados.

El Oficial de Registro procede a la guarda de la carpeta en un armario ignífugo ubicado en el segundo nivel de la RA correspondiente.

En caso de que uno o más documentos no cumplan los requisitos necesarios, existan dudas en cuanto a la validez de los documentos de identidad o la correspondencia entre el documento presentado y su titularidad, la documentación será devuelta al solicitante que deberá iniciar un nuevo de identificación dentro del plazo de vigencia de su solicitud que es de 30 días y presentar los documentos actualizados ante la RA.

Si la Solicitud es rechazada o dada de baja por falta de identificación, la aplicación le informará la condición al Solicitante por medio de un correo electrónico.

Para los casos de re-emisión, el Oficial de Registro podrá requerir, ante dudas, respecto de la verificación realizada con anterioridad, que el Solicitante o Suscriptor se presente nuevamente para acreditar identidad.

- **Resultado del procedimiento**

a) En caso de aceptación:
   - Solicitud aprobada.
   - Acuerdo con Suscriptores firmado.
   - Carpeta de identificación del Solicitante o Suscriptor en la RA Central.

b) En caso de rechazo:
   - Solicitud rechazada.

3.2.3. Autenticación de la identidad de persona física

Este proceso tiene como requisito previo la elaboración de la solicitud del certificado digital y la creación del par de claves criptográficas, son parte del Ciclo del certificado y se describen en " 4.1.2.1 Certificado de Persona Física para firma digital y para autenticación" de la CP.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Planificado. Urgencia alta.

Se realiza solo en horario laboral.

- **Roles que participan en el procedimiento**
  a) Solicitante o suscriptor
  b) Oficial Identificador
  c) Oficial de Registro

- **Acción que pone en marcha el proced--imiento**

Solicitud de identificación de una persona física a la RA.

- **Tareas a realizar por cada uno de los roles que actúan**

El solicitante presenta la siguiente documentación en original y copia:

- Exhibición del documento original de identidad expedido por el Departamento de Identificación de la Policía o Nacional el cual deberá estar vigente en el momento de su presentación
- Acuerdo con Suscriptores
- Solicitud de firma digital
- Comprobante de pago

El Solicitante será atendido por el Oficial Identificador, quien verificará su identidad. Este revisará que:

El documento de identidad presentado sea válido, que sea el mismo tipo y número que se indicó en la solicitud de certificado y que la foto coincida con la persona que tiene enfrente y comprueba que la información suministrada concuerda con los datos oficiales mediante la consulta a bases de datos oficiales de verificación de identidad.

El nombre de la persona física que obra en la Solicitud sea el mismo que en el que figura en la Solicitud sea igual al del documento de identidad.

Si la identificación ha sido aprobada, el Solicitante firma dos ejemplares impresos del "Acuerdo con Suscriptores", quedando uno en poder del Solicitante.

El Oficial Identificador devuelve los originales de todos los documentos al Solicitante y conserva los duplicados, como respaldo del proceso de identificación.

Luego un Oficial de Registro cargará en la aplicación de la RA la confirmación de los documentos recibidos y determinará la aceptación o rechazo de la Solicitud.

En caso de aprobar la Solicitud, firmará la misma con su certificado habilitado en la aplicación de la RA.

Finalmente, en caso de aprobación, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

El Oficial de Registro, arma la carpeta de respaldo de la identificación de la persona física Solicitante. Esta contiene la Solicitud de Certificado firmada, los duplicados de todos los documentos presentados y el Acuerdo con Suscriptores firmado.

En caso de que uno o más documentos no cumplan los requisitos necesarios, existan dudas en cuanto a la validez de los documentos de identidad o la correspondencia entre el documento presentado y su titularidad, la documentación será devuelta al solicitante que deberá iniciar un nuevo proceso de identificación dentro del plazo de vigencia de su solicitud que es de 30 días y presentar los documentos actualizados ante el personal de la RA.

Si la Solicitud es rechazada o dada de baja por falta de identificación, la aplicación le informará la condición al Solicitante por medio de un correo electrónico.

Para los casos de re-emisión, el Oficial de Registro, podrá requerir, ante dudas, respecto de la verificación realizada con anterioridad, que el Solicitante/Suscriptor se presente nuevamente para acreditar identidad.

- **Resultado del procedimiento**

En caso de aceptación:

- Solicitud aprobada.
- Acuerdo con Suscriptores firmado.
- Carpeta de identificación del Solicitante/Suscriptor en la RA Central

En caso de rechazo;

- Solicitud rechazada.
- Correo electrónico de notificación de rechazo.

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, incluyendo la generación de un nuevo par de claves y también el envío de la nueva solicitud y la presentación frente a la RA para validar su identidad.

3.4. Identificación y autenticación para solicitudes de revocación

El requerimiento de revocación de los certificados digitales se describe en "3.4. Requerimiento de revocación" de la CP.

El requerimiento de revocación podrá ser iniciado por el Suscriptor o por la RA. La RA podrá iniciar el requerimiento de oficio o por decisión del Certificador, cuando se produzcan las causas indicadas en "3.4 - Requerimiento de revocación" de la CP.

Luego de hecho el requerimiento, deberá efectivizase la revocación, como se describe en "4.9. Revocación y supensión" de la CP.

3.4.1. Procedimiento para requerir la revocación

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Poco frecuente. No planificado. Urgencia muy alta.

- **Roles que participan en el procedimiento**

a) Suscriptor

b) Oficial de Registro

c) CA

- **Acción que pone en marcha el procedimiento**

En el caso del Suscriptor, puede iniciar el proceso accediendo al sitio web correspondiente o presentarse ante la RA para solicitarlo.

El representante legal, administrador o apoderado, si se trata de una persona jurídica, puede iniciar el proceso accediendo al sitio web correspondiente o presentarse ante la RA para solicitarlo.

En caso de detección de alguna causa de revocación también podrán solicitarla:

- La RA
- La AA
- La Autoridad Judicial competente.
- El PSC.

Estas causas podrán ser:

a) 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.

a) 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.

b) CODE100 S.A. determine que los procedimientos de emisión y/o verificación han dejado de ser seguros.

c) La Organización que haya adoptado el uso de certificados de firma digital emitidos por la CA, notifique a la RA que la información contenida en el certificado ha dejado de ser exacta.

d) Fuere solicitado por resolución judicial o de la AA

e) CODE100 S.A. determine que el certificado dejó de cumplir con las políticas y normas legales y reglamentarias de la Infraestructura de Clave Pública del Paraguay.

f) 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.

g) 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 SA.

h) Por cambio en los atributos de un certificado, aun cuando hubieran sido válidos al tiempo de su emisión.

i) Por cese de la existencia de la Persona Jurídica, comunicada fehacientemente por el representante legal de la misma a CODE100 S.A.

j) Por cese de la habilitación del PSC.

k) Por haberse resuelto el contrato que CODE100 S.A. hubiera suscripto con la Organización a la cual perteneciese el Suscriptor, o lo convenido entre las partes, en el caso que corresponda.

- **Tareas a realizar por cada uno de los roles que actúan**

a) Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del PSC desde:

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

b) La persona que inicia la revocación se debe identificar en la aplicación con su Documento de Identidad y su Clave o PIN de revocación, y procede a enviar la solicitud de revocación, la que es procesada de inmediato.

c) Este sitio está disponible 7 días de la semana, las 24 horas, los 365 días del año.

d) En caso que el suscriptor se presente ante la RA, esta controlará las causas de revocación manifestadas por el suscriptor y en caso de que presente documentación, el Oficial de Registro sacara duplicado de lo presentado.

e) El suscriptor firma la documentación entrega al oficial de registro.

f) El oficial de registro firma la documentación recibida.

g) En la aplicación de la RA seleccionara la solicitud correspondiente al certificado que se autoriza revocar y generara el requerimiento en la aplicación.

h) El Oficial de Registro asentará en el libro de actas de la RA el requerimiento de revocación.

i) El Suscriptor recibirá un correo electrónico de la aplicación informando la revocación del certificado.

j) La RA es notificada por la aplicación para hacer el proceso de registro y archivo como respaldo de la acción realizada.

k) En el caso que el Solicitante/Suscriptor no contara con el PIN, lo podrá solicitar en el portal del suscriptor

l) La aplicación, en forma automática, le devolverá en su correo electrónico al Solicitante/Suscriptor, el PIN para que pueda realizar la revocación.

m) En caso de tratarse de personas o entidades habilitadas para solicitar la revocación y que no cuenten con el PIN de revocación correspondiente, deberán comunicarse a los contactos establecidos por CODE100 S.A. en "1.4 Contactos de la CP", solicitar la revocación al Responsable de la RA de la siguiente manera:

Autoridad de Aplicación: mediante notificación fehaciente

Autoridad Judicial Competente: mediante oficio judicial.

En todos los casos enunciados en este punto se dejara constancia en el libro de Actas del motivo de la revocación y la misma será autorizadas por el Responsable Legal de CODE100 SA.

n) En los casos de que no se pueda verificar las condiciones para proceder a la revocación, la solicitud de revocación será rechaza y comunicado al correo electrónico informado por el suscriptor al momento de la solicitud.

- **Resultado del procedimiento**

En caso de verificar las condiciones para una revocación

- Pedido de Revocación solicitada.
- Notificación de la revocación al Solicitante.
- Notificación de la revocación a la RA.
- Actualización del Libro de Actas de la RA.
- Envío de PIN de revocación, si corresponde.

En caso de no poder verificar las condiciones para una revocación

- Solcitud de Revocación Rechazada.
- Correo de notificación de Solcitud de revocación Rechazada.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de certificado

El proceso de creación de la solicitud de certificado digital, incluye la generación del par de claves criptográficas que formarán parte del certificado.

4.1.1 Solicitud de certificado para persona física

Los requerimientos están detallados en "3.2.3 Autenticación de identidad de Persona Física" de la CPS.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

- **Roles que participan en el procedimiento**

a) Solicitante

- **Acción que pone en marcha el procedimiento**

Acceso del Solicitante al sistema, acreditando su identidad.

- **Tareas a realizar por cada uno de los roles que actúan**

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el Solicitante, quien luego, debe acreditar fehacientemente su identidad según se indica en "3.1.9. - Autenticación de la identidad de personas físicas".

Para poder efectuar la Solicitud de un certificado de persona física, 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.

- En caso de contar el Solicitante con un dispositivo criptográfico propio, de los modelos homologados por el Certificador, deberá colocarlo al inicio de la sesión.
- La aplicación, mostrara el formulario de Solicitud de persona física deberá ser completado por el solicitante.
- El sistema a continuación desplegará las RA, debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación. Habiendo confirmado los datos de la solicitud y elegido donde realizar la identificación, como medida de seguridad, se envía la solicitud al correo electrónico del titular declarado en la misma, solicitando la confirmación.
- El Solicitante recibe en el mail informado el pedido de confirmación y lo abre y envía la confirmación a la aplicación de solicitud.
- Únicamente al ser confirmada la recepción del correo electrónico la aplicación le mostrara la continuación del formulario de Solicitud.
- La aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generará el par de claves criptográficas asimétricas.
- El Solicitante al generar las claves por hardware, el dispositivo criptográfico deberá ser provisto por el suscriptor, y deberá establecer la clave de acceso al dispositivo criptográfico y el mismo debe estar dentro de los modelos especificados en la lista de los dispositivos homologados por CODE100 S.A. Las claves de los suscriptores que cuenten con dispositivos criptográficos externos removibles deberán estar protegidas por tres factores de seguridad: 1) mediante la posesión del dispositivo por el suscriptor, 2) mediante una contraseña de acceso al dispositivo criptográfico definida por el propio suscriptor, 3) la contraseña de la clave privada definida por el propio suscriptor.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10 sobre el dispositivo criptográfico que posee elSolicitante.
- Generadas las claves, la aplicación del Certificador 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 del certificado.

- Cumpliendo el Solicitante con presentarse en la RA elegida o ser visitado por un Oficial Identificador 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 Identificador, este verifica que la generación del requerimiento del certificado de firma digital es realizada en un dispositivo criptográfico homologado por CODE100 S.A. y previo al procesamiento de la solicitud se realiza una segunda revisión a la documentación recibida por el Oficial de Registro.
- Si la Solicitud es rechazada, se le informa este hecho al Solicitante, en su dirección de correo electrónico.
- Se establece el plazo máximo de cinco días hábiles para la tramitación de la solicitud del certificado, contados a partir de haberse verificado la identidad del solicitante y admitida la solicitud. En caso que la CA supere el plazo máximo establecido para la tramitación de la solicitud, deberá informar al solicitante de las causas que motivaron la demora y el nuevo plazo en el que se tramitará la solicitud. En caso que el interesado opte por desistir de su solicitud por el motivo expuesto en la CA tendrá previsto un procedimiento de reembolso de lo abonado.

➢ **Resultado del procedimiento**

Si fue exitoso:

- El Solicitante generó el par de claves criptográficas en un dispositivo criptográfico homologado.
- La aplicación generó la solicitud pendiente de identificación.
- Se informó al Solicitante el pin de revocación.
- El Sistema le envió al Solicitante un recordatorio para el proceso de identificación.

Si se rechazó:

- El Solicitante fue notificado respecto al rechazo de su Solicitud.

4.1.2. Solicitud de certificado para persona jurídica

Los requerimientos están detallados en "3.2.2 Autenticación de identidad de Persona Jurídica" de la CPS.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

- **Roles que participan en el procedimiento**

a) Solicitante, persona jurídica, iniciado a través de su representante, administrador o apoderado.

- **Acción que pone en marcha el procedimiento**

Acceso del solicitante en su carácter de representante legal, administrador o apoderado al sistema, acreditando su identidad y el registro los datos de la persona jurídica solicitante.

- **Tareas a realizar por cada uno de los roles que actúan**

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 según se indica en "3.2.2 Autenticación de identidad de Persona Jurídica" de la CP.

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 propia y exclusiva del solicitante 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.
- 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.
- La aplicación del PSC verifica que la estación de trabajo del Solicitante cumple con los requerimientos técnicos mínimos.
- Se debe contar el Solicitante con un dispositivo criptográfico propio y deberá colocarlo al inicio de la sesión.

- La aplicación le presenta la pantalla con el formulario de Solicitud de Certificado de Persona Jurídica. El solicitante completara este formulario y confirmará los datos del mismo.
- A continuación le solicita todos los datos del Solicitante en su calidad de representante legal, administrador o apoderado de la persona jurídica.
- Completada la Solicitud, el Solicitante deberá confirmar todos los datos presentes en la misma.
- El sistema a continuación desplegará las RA debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación.
- Habiendo confirmado los datos de la Solicitud y elegido el lugar para la identificación, como medida de seguridad, se la envía al correo electrónico declarado en la solicitud, solicitando la confirmación.
- El Solicitante recibe en el mail informado el pedido de confirmación y lo abre y envía la confirmación a la aplicación de solicitud.
- Únicamente al ser confirmada la recepción del correo electrónico la aplicación le mostrara la continuación del formulario de Solicitud.
- La aplicación 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 sobre un dispositivo criptográfico, el Solicitante debe contar con la clave de acceso al dispositivo criptográfico y podrá realizar la generación en el mismo.
- Generadas las claves, la aplicación del Certificador 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 ubicación de la identificación 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.
- Cumpliendo el Solicitante con presentarse en la RA elegida o ser visitado por un Oficial Identificador para su identificación, la aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de los requerimientos para la verificación de la identidad del Solicitante y al

cumplimiento de los requisitos específicos en relación a las características del certificado digital solicitado.

- En caso de ser visitado por un Oficial Identificador, este verifica que la generación del requerimiento del certificado de firma digital es realizada en un dispositivo criptográfico homologado por CODE100 S.A. y previo al procesamiento de la solicitud se realiza una segunda revisión a la documentación recibida por el Oficial de Registro.
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.

➢ **Resultado del procedimiento**

Si fue exitoso:

- El Solicitante generó el par de claves criptográficas en un dispositivo criptográfico homologado.
- La aplicación generó la solicitud de certificado de persona jurídica pendiente de identificación.
- Se informó al Solicitante el pin de revocación.
- El Sistema le envió al Solicitante un recordatorio para el proceso de identificación.

Si fue rechazado:

- Se informa al Solicitante el rechazo de su Solicitud

4.1.3. Solicitud de renovación de certificado de Persona Física

No aplica.

4.1.4. - Solicitud de renovación de certificado de Persona Jurídica

No aplica.

4.2. Emisión del certificado

El certificado se emite y se coloca en el portal del suscriptor, luego de cumplido el proceso de identificación y autenticación y aprobada la Solicitud de emisión de certificado por la RA y abonado el arancel de emisión y/o re-emisión.

El Portal del Suscriptor se encuentra en:

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

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

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia alta.

- **Roles que participan en el procedimiento**

a) CA.

- **Acción que pone en marcha el procedimiento**

Información ingresada por la RA sobre aprobación de la solicitud y pago del arancel.

- **Tareas a realizar por cada uno de los roles que actúan**

La aplicación de la CA verifica la firma digital de la aprobación realizada por la RA a la Solicitud de emisión.

La aplicación de la CA remite el requerimiento con la clave pública del solicitante, en formato PKCS#10, al Servicio de Certificación de la CA.

El Servicio de Certificación de la CA emite el correspondiente certificado, firmándolo digitalmente con su clave privada.

La CA pone el certificado en el área de comunicaciones con la aplicación del Certificador.

La aplicación del PSC coloca el certificado en el Portal del Suscriptor, a disposición de su titular.

El Portal del Suscriptor se encuentra en:

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

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

Le comunica al Solicitante o Suscriptor la disponibilidad de su certificado por correo electrónico.

La aplicación de la CA, una vez que se emitió el certificado, eliminará automáticamente el requerimiento PKCS#10 asociado a ese certificado con el fin de evitar que se genere un nuevo certificado con dicho requerimiento.

El proceso continúa con "4.4. Aceptación del Certificado" de la CP.

- **Resultado del procedimiento**

Se emitió el certificado, firmado con la clave privada de la CA, y se lo puso a disposición del solicitante que se convierte en suscriptor.

4.3. Aceptación del certificado

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Numerosas veces por día. Urgencia baja.

- **Roles que participan en el procedimiento**

a) Suscriptor

- **Acción que pone en marcha el procedimiento**

Aviso de emisión del certificado, enviado por la aplicación del Certificador y recibido por el suscriptor.

- **Tareas a realizar por cada uno de los roles que actúan**

El Portal del Suscriptor se encuentra en:

http://www.CODE100.com.py/firma-digital/portal-suscriptor.htm |

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

El suscriptor descarga su certificado desde el portal, almacenándolo en el dispositivo criptográfico si dispone de él o en el disco de su computador.

El suscriptor debe controlar el contenido del certificado.

Si el contenido es incorrecto debe revocar el certificado con su pin de revocación desde el mismo portal o en caso contrario informar de inmediato sobre cualquier error a la RA, para que ésta solicite en forma urgente la revocación.

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 de la puesta a disposición en el portal del suscriptor del certificado a su nombre

Si no encuentra ni comunica error, se entiende que el certificado es correcto, el suscriptor acepta todas sus obligaciones y derechos desde el momento de su emisión según se establecen en la CP y en el Acuerdo con suscriptor que obra en poder del Solicitante.

- **Resultado del procedimiento**

Certificado aceptado en poder del suscriptor, en condiciones de ser usado según lo especificado en la CP.

Si los datos son incorrectos, el Certificado es revocado.

4.4. Suspensión y Revocación de Certificados

4.4.1. Causas de revocación

Las causas contempladas están expuestas en "4.9.1 Circunstancias para la revocación" de la CP.

4.4.2. Autorizados a solicitar la revocación

Los actores listados en "4.9.2 Quien puede solicitar Revocación" de la CP podrán presentar el pedido de revocación.

4.4.3. Procedimientos para la solicitud de revocación

Para solicitar la revocación de un certificado, se seguirá lo indicado en " 4.9 Revocación y suspensión".

En el presente punto se trata el procesamiento de esa solicitud, a los efectos de materializar la revocación solicitada.

- **Frecuencia, oportunidad y urgencia**

Disponibilidad permanente. Pocas veces por día. Urgencia extrema.

- **Roles que participan en el procedimiento**

b) Solicitante

c) Oficial de Registro

d) CA.

- **Acción que pone en marcha el procedimiento**

Solicitud de revocación de certificado, iniciada por el mismo suscriptor o el Oficial de la RA, la que es recibida por la CA.

- **Tareas a realizar por cada uno de los roles que actúan**

a) El solicitante ingresa al portal y con su pin de revocación y genera la solicitud.

b) El Oficial de Registro selecciona el certificado a revocar y genera la solicitud de revocación.

c) La aplicación de la CA procesa inmediatamente la solicitud de revocación y remite el requerimiento al Servicio de Certificación de la CA.

d) El Servicio de Certificación de la CA revoca el correspondiente certificado.

e) La aplicación de la CA notifica al suscriptor y a la RA, por correo electrónico acerca de la revocación del certificado.

f) La CA incluye la información del certificado revocado en la nueva lista de certificados revocados. Cuando se cumplen las 24 horas de publicada la última CRL se publica la nueva CRL con el nuevo certificado revocado.

g) En caso de tratarse de personas o entidades habilitadas para solicitar la revocación y que no cuenten con el PIN de revocación correspondie nte, deberán comunicarse a los contactos establecidos por CODE100 S.A. en "1.4 Contactos de la CP", solicitar la revocación al Responsable de la RA de la siguiente manera:

AA: mediante notificación fehaciente.

Autoridad Judicial Competente: mediante oficio judicial.

En todos los casos enunciados en este punto se dejara constancia en el libro de Actas del motivo de la revocación y la misma será autorizadas por el Responsable Legal de CODE100 SA.

- **Resultado del procedimiento**

Certificado digital revocado, de acuerdo con la solicitud.

La RA conservará como documentación probatoria la solicitud de revocación y el material probatorio vinculado.

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

4.4.4. Plazo para la solicitud de revocación

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

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

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

En caso que el suscriptor se presente ante la RA, esta controlará las causas de revocación manifestadas por el suscriptor y en caso de que presente documentación, el Oficial de Registro realizará un duplicado de la documentación presentada.

El Oficial de Registro verificará que se cumplan las condiciones para realizar una solicitud de revocación.

En la aplicación de la RA el Oficial de Registro seleccionará la solicitud correspondiente al certificado que se autoriza revocar y generará el requerimiento en la aplicación.

El Oficial de Registro asentará en el libro de actas de la RA el requerimiento de revocación.

El Suscriptor recibirá un correo electrónico de la aplicación informando la revocación del certificado.

4.4.5. Causas de suspensión

El estado de suspensión no es admitido.

4.4.6. Autorizados a solicitar la suspensión

El estado de suspensión no es admitido.

4.4.7. Procedimientos para la solicitud de suspensión

El estado de suspensión no es admitido.

4.4.8. Límites del periodo de suspensión de un certificado

El estado de suspensión no es admitido.

4.4.9. Frecuencia de emisión de listas de certificados revocados

La CA 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.

Para poder realizar la publicación CODE100 S.A. ha desarrollado un servicio CODE100PUB que está disponible las 24 horas para realizar la publicación de la CRL.

Este servicio se encarga de buscar, distribuir y publicar en el servidor principal de publicación y servidor secundario la última CRL emitida por el servicio de "Certificate Service" diariamente. Cuenta además con CODE100MON que es otro servicio encargado

de supervisar que los servicios del PSC tales como CODE100PUB se cumplan con normalidad.

Este servicio se encarga de:

Verificar que las publicaciones se realicen con la periodicidad necesaria.

Verificar que las CRL estén vigentes.

Que las CRL se copien en los puntos de distribución correspondientes según lo especificado en el perfil de los certificados.

Que los sitio de publicación estén respondiendo correctamente a las peticiones HTTP y HTTPS.

Notificar por correo electrónico al Responsable de Seguridad la detección de cualquier incidente.

4.4.10. Requisitos para la verificación de la lista de certificados revocados

Para determinar el estado de validez de un certificado, se debe obtener la CRL vigente, verificar su integridad controlando la validez de su firma y constatar la inclusión o no del certificado en cuestión.

En los repositorios descriptos en "2.2 Publicación de Información de Certificación" se conserva únicamente la última CRL emitida. Las versiones de CRLs emitidas previamente son mantenidas en los archivos internos del Certificador

Si no se pudiera obtener una CRL actualizada, quien busca la verificación deberá optar entre rechazar el documento firmado digitalmente, aceptarlo bajo exclusiva responsabilidad de quien consulta o postergar la decisión hasta obtener una CRL actualizada.

Todas las aplicaciones habilitadas para el uso de los certificados emitidos por CODE100 S.A. cuentan con servicio de verificación automática de los certificados.

Las aplicaciones habilitadas por CODE100 S.A se encuentran publicadas en la url:

http://www.CODE100.com.py/firma-digital/aplicaciones.pdf

Las mismas verifican en forma automática el estado de validez de los certificados utilizados por los suscriptores.

4.4.11. Disponibilidad del servicio de consulta sobre revocación y de estado del certificado

Las respuestas a las consultas sobre el estado de un certificado, por medio del servicio de verificación en línea del estado de los certificados, denominado Online Certificate Status Protocol (OCSP) o Protocolo en Línea del Estado de los Certificados.

Adicionalmente a la lista de certificados revocados, la CODE100 provee un servicio de verificación en línea del estado de los certificados
Este servicio se provee por medio del sitio web "ac1.code100.com.py/ocsp/".
Las respuestas de este servicio son firmadas con la clave del certificado OCSP.

4.4.12. Requisitos para la verificación en línea del estado de revocación

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de un certificado digital y representa una alternativa al servicio de CRLs, el que también estará disponible. Este servicio se provee por medio del sitio web "ac1.code100.com.py/ocsp".

Usando este protocolo se consulta, por medio del número de serie de un certificado digital, al repositorio de certificados digitales de la AC de CODE100, detectando e informando el resultado de la consulta.

El resultado de la consulta estará firmado con la clave del certificado OCSP correspondiente.

4.4.13. Otras formas disponibles para la divulgación de la revocación

No hay otras formas disponibles.

4.4.14. Requisitos para la verificación de otras formas de divulgación de revocación

No aplicable.

4.4.15. Requisitos específicos para casos de compromiso de claves

Todas las situaciones que involucren el compromiso de la clave privada del suscriptor, el suscriptor deberá revocar su certificado. Podrá hacerlo por alguna de las vías indicadas en "3.4. Requerimiento de revocación" de la CP.

4.5. Procedimientos de Auditoría de Seguridad

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. Lo mismo hace las RA, dentro de los alcances de sus acciones.

Estos registros de auditoría son utilizados para las tareas de monitoreo habitual del funcionamiento de los sistemas y procesos, para posibles auditorías internas y para las auditorías que realiza la AA.

Los registros de auditoría son analizados por el servicio CODE100MON en las tareas de monitoreo habitual del funcionamiento de los sistemas, las aplicaciones y los procesos.

Con el propósito de mantener la seguridad de los sistemas, el Coordinador de Seguridad realiza evaluaciones periódicas sobre los informes de CODE100MON, servicio que registra en forma automática las alteraciones en el funcionamiento de la instalación.

La información relacionada al registro de eventos se encuentra centralizada en el servidor de monitoreo y es administrado con un software de gestión de eventos. Éste se encargará de recopilar todos los eventos de seguridad, aplicación, sistema y firewalls de los equipos que conforman la plataforma tecnológica de CODE100 S.A.

Estos eventos son monitoreado diariamente por el Responsable Técnico.

El software de monitoreo se encuentra configurado para realizar notificaciones en casos de alertas por correo electrónico al Responsable Técnico y al Coordinador de Seguridad.

Los registros no electrónicos de acceso físico por parte de solicitantes, suscriptores o terceros son registrados manualmente en el libro de registros de ingresos de la CA de CODE100 S.A., las RA y Sitio Alterno.

Asimismo, se mantendrán registros no informatizados de toda aquella información soportada en papel.

4.6. Archivo de registros de eventos

El PSC genera, mantiene y conserva registros de eventos sobre cada una de las siguientes actividades que comprenden los componentes del proceso de certificación. La información registrada abarca:

Fecha y hora del registro

Número de serie o secuencia del registro

Tipo de registro

Fuente del registro

Identificación de la entidad que efectuó el registro

Administración del ciclo de vida de las claves criptográficas	a) Generación y almacenamiento de las claves criptográficas del certificador b) Resguardo y recuperación de las claves criptográficas del certificador c) Utilización de las claves criptográficas del certificador d) Archivo de las claves criptográficas del certificador e) Retiro de servicio de datos relacionados con las claves criptográficas f) Destrucción de claves criptográficas del certificador 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 re-emisión 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 certificador 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 y de los oficiales de registro. b) El certificador registra el número de serie del dispositivo que se entrega y quien lo recibe. c) El responsable técnico registra la inicialización del dispositivo

	criptográfico.
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. o personal relacionado con el proceso de certificación h) Accesos a los componentes del sistema de la CA i) Eventos o situaciones no previstas

La información relacionada al registro de eventos se encuentra centralizada en el servidor de monitoreo.

Este se encargará de recopilar todos los eventos de seguridad, aplicación, sistema y "firewalls" de los equipos que conforman la plataforma tecnológica de CODE100 S.A.

Estos eventos son monitoreados diariamente por el Responsable Técnico.

El software de administración de eventos se encuentra configurado para realizar notificaciones en casos de alertas por correo electrónico al Responsable Técnico y al Coordinador de Seguridad.

Los registros no electrónicos de acceso físico por parte de solicitantes, suscriptores o terceros son registrados manualmente en el libro de registros de ingresos de la CA de CODE100 S.A., RA y Sitio Alterno.

El Jefe de Área registra:

En los Libros de Actas de la CA las tareas de resguardo.

En el Libro de Actas de Contingencia la ceremonia inicial, los controles periódicos, etc. la fecha y un breve resumen de las tareas realizadas y ingreso al Sitio de Máxima Seguridad de Contingencia a las personas no incluidas en la Lista de Contactos Primarios y Sustitutos para la Contingencia (que deben ingresar a este Sitio), el tipo de evento, la fecha y un breve resumen del Inventario de Bienes y Servicios realizado.

El Oficial de Registro registra en el libro de actas de la CA se encuentra resguardado en el cofre de seguridad ubicado en el sitio de máxima seguridad de CODE100 S.A.

El libro de actas del sitio de contingencia se encuentra resguardado en el cofre de seguridad ubicado en el sitio de máxima seguridad de contingencia.

4.7. Cambio de claves criptográficas

Las claves criptográficas de la CA son generadas con motivo la habilitación de la presente CP y tendrán una duración de 10 años.

El cambio del par de claves criptográficas de la CA, dará origen a la emisión de un nuevo certificado, por parte de la CA Raíz de la República del Paraguay operada por la AA.

Seis meses antes del vencimiento previsto del certificado de la CA se solicitará la renovación de la habilitación de la CP y el certificado correspondiente.

4.8. Plan de contingencia, Recuperación Frente a Desastres y Continuidad del Negocio

El Plan de Contingencia, Recuperación Frente a Desastres y Continuidad del Negocio de CODE100 S.A. como PSC establece los procedimientos y actividades relacionados con el servicio de certificación de firma digital y será de aplicación desde el momento de la declaración de la emergencia hasta la restauración de la operatoria normal.

- **Frecuencia, oportunidad y urgencia**

Un año antes del vencimiento del certificado. Urgencia Alta.

- **Roles que participan en el procedimiento**

a) Jefe de Área

b) Responsable Técnico

- **Acción que pone en marcha el procedimiento**

Al certificado de la CA solo le queda un año de vigencia.

- **Tareas a realizar por cada uno de los roles que actúan**

a) El Responsable Técnico inicia el servicio de emisión de Certificados
b) El Responsable Técnico solicita el nuevo certificado de la CA con generación de nuevo par de claves.
c) El Servicio de Emisión de Certificados genera un nuevo requerimiento de solicitud de certificado.
d) El Responsable Técnico copia el requerimiento asociado al nuevo par de claves generadas y lo copia en un CD.
e) El Responsable Técnico entrega el CD con el nuevo requerimiento al Responsable de Firma digital
f) El Jefe de Área envía el requerimiento a la AA
g) La AA envía el nuevo certificado
h) El Jefe de Área Autoriza la instalación
i) El Responsable Técnico completa el proceso de instalación del nuevo certificado
j) El Jefe de Área registra en el libro de actas las tareas realizadas.

- **Resultado del procedimiento**

Certificado de CA Renovado

Registro en libro de Actas del nuevo certificado.

4.9. - Plan de Cese de Actividades

El Plan de Cese de Actividades de CODE100 S.A., contempla las estrategias y procedimientos a seguir desde la decisión de suspender en forma definitiva el servicio de certificación hasta la inhabilitación lógica y física de la CA.

Más información se encuentra en el documento "Plan de Cese de Actividades de CODE100 S.A."

5. CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

5.1. Controles de seguridad física

Los sistemas centrales de la CA se encuentran en el Sitio de Máxima Seguridad (SMS) de CODE100 S.A., el cual cuenta con controles de seguridad física que protegen las instalaciones informáticas de la CA y garantizan la continuidad de sus operaciones.

Más información se encuentra en el documento "Plan de Seguridad".

5.2. Controles Funcionales

Los controles funcionales son realizados por personal de CODE100 S.A. sobre todos los roles que componen la CA, verificando el cumplimiento de las responsabilidades de cada uno de ellos, de acuerdo a lo establecido en la CP y en el documento Roles y Funciones.

Los roles son asignados por el Jefe de Área, respetando los siguientes criterios:

a) Cada uno de los roles tiene un titular asignado y un sustituto.

b) Los roles son asignados a personal que cumple funciones en CODE100 S.A.

En el caso de la CA, las RA se realizan controles funcionales, verificando el cumplimiento de las responsabilidades y procedimientos:

a) La información de la solicitud ingresada por el Solicitante y la aprobación en la base de datos se encuentra firmada digitalmente por la RA respectiva, impidiendo cualquier intento de manipulación de datos.

b) Las firmas digitales de las RA son verificadas por las aplicaciones de la CA, como paso previo a la emisión de un certificado.

c) Las RA deben verificar los atributos unívocos de la solicitud (tipo y número de documento) junto con el resto de la información.

d) Las RA son responsables de cotejar los datos de la solicitud con la información obrante en sus registros y la documentación de respaldo.

e) Se realizan revisiones periódicas para cotejar las solicitudes y los certificados emitidos con la documentación de respaldo correspondiente.

f) Previo a la emisión, las aplicaciones de la CA verifican la congruencia entre la información de la solicitud y del certificado.

g) Antes de la puesta en producción de una nueva versión de las aplicaciones de la CA de cualquier otro software incluido en el equipo, personal de CODE100 S.A. somete al sistema a pruebas de aceptación que determinan la confiabilidad del producto.

h) Los servidores de la CA son monitoreados para asegurar que no se incluyeron o reemplazaron archivos no autorizados dentro del sistema, por algún mecanismo basado en el cálculo y comparación de la función "hash" de los archivos del equipo.

i) La información de solicitudes y aprobaciones de la base de datos se encuentra firmada digitalmente por la RA respectiva, impidiendo cualquier intento de manipulación de datos. Las firmas digitales de las RA son verificadas por las aplicaciones de la CA como paso previo a la emisión de un certificado.

j) Se registran "logs" de todos los accesos y transacciones de la base de datos.

k) Existen controles de consistencia sobre la base de datos que permiten determinar si la información es completa y correcta.

l) Las aplicaciones de la CA son monitoreadas constantemente y se envían mensajes de alerta.

m) La Mesa de Ayuda de CODE100 S. A. está capacitada para asistir a todos los suscriptores y puede contactarse mediante correo electrónico o por teléfono, tal como se describe en el documento CP.

n) El sistema es monitoreado constantemente y se envían mensajes de alerta.

o) Si el problema no puede ser resuelto en un plazo de 24 horas, se trasladan las operaciones al sitio de contingencia.

p) En caso que el rol de Responsable Técnico detecte problemas en el HSM que no puedan ser resueltos en el plazo de 16 horas se trasladan las operaciones al sitio de contingencia.

q) La emisión de las CRLs es monitoreada por el servicio CODE100MON, encargado en notificar por correo electrónico al responsable de monitoreo.

r) La información de cada CRL es cotejada con la CRL precedente.

s) Se realizan revisiones periódicas para cotejar que todos los certificados revocados estén incluidos en la CRL correspondientes.

t) Antes de la puesta en producción de una nueva versión de las aplicaciones de la CA o de cualquier otro software incluido en el equipo, personal de CODE100 S.A. somete al sistema a pruebas de aceptación que determinan la confiabilidad del producto.

5.3. Controles de seguridad del personal

Los controles de seguridad del personal que desempeña los roles que componen la CA, serán los establecidos por CODE100 S.A. e implementados a través de su Responsable de Recursos Humanos. Se efectúa un previo análisis y seguimiento de los antecedentes laborales del personal a través de su "Curriculum Vitae" y evalúa la idoneidad del aspirante mediante una valoración psicotécnica. Además, CODE100 S.A. realiza una evaluación anual del desempeño de todo su personal.

5.3.1. Antecedentes laborales, calificaciones, experiencia e idoneidad del personal

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

Todos los antecedentes personales y profesionales son evaluados antes de la asignación de una persona a un rol en estos servicios por el Jefe de Área y el Responsable de Recursos Humanos. Participarán también cuando se trate de personal para el rol de Oficial de Registro.

Todo el personal de la CA de CODE100 S.A. cumple o ha cumplido un Proceso de Selección previo a su incorporación que provee una razonable seguridad acerca de la confiabilidad y competencia de su personal para el adecuado cumplimiento de sus roles y funciones y que incluye los siguientes controles:

a) El Responsable de Recursos Humanos de CODE100 S.A. conserva los certificados de falta de antecedentes penales de los candidatos en los correspondientes legajos del personal. Sólo son considerados quienes no poseen ningún antecedente negativo. También conserva constancia de los antecedentes de competencia, idoneidad y laborales de los candidatos en los correspondientes legajos de personal y en los sistemas de evaluación de desempeño, conforme a los requisitos establecidos para la contratación o designación en los regímenes aplicables.
b) El Responsable de Recursos Humanos de CODE100 S.A. verifica de la aptitud de los candidatos mediante el chequeo de los antecedentes y referencias presentadas, entrevistas personales u otros mecanismos de selección adecuados para su precalificación.
c) La selección entre los candidatos que hayan aprobado la prueba de aptitud del punto precedente está a cargo del Jefe de Área de CODE100 S.A.
d) Finalizado el Proceso de Selección, los candidatos seleccionados son contratados o designados en los roles respectivos por el Jefe de Área.
e) El Responsable de Recursos Humanos de CODE100 S.A. comunica por escrito el nombramiento a cada uno de los interesados y les hace firmar el "Acuerdo de

Confidencialidad" mencionado en el punto "1.1. Cumplimiento" del presente documento y cuyo modelo se encuentra en el punto "8. Acuerdo de Confidencialidad" del Manual de Procedimientos de Certificación (Reservado).

f) Toda la documentación de este proceso de selección, incluidos los "Acuerdos de Confidencialidad" oportunamente firmados son conservados en los archivos de la CA de CODE100 S.A. bajo la custodia del Responsable de Seguridad Informática.

Verificaciones de aptitud

a) Análisis y evaluación de los Certificados de falta de antecedentes penales, de aptitud laboral y personal presentados por los candidatos.

b) Comprobación de integridad y veracidad de la Hoja de Vida (Currículum Vitae) de los aspirantes.

c) Constatación de las aptitudes académicas y profesionales de los aspirantes obrantes en sus respectivas Hojas de Vida, según corresponda.

d) Verificación de la identidad de los aspirantes mediante la inspección de sus respectivos DNI o Pasaportes, según corresponda.

e) Verificación de Crédito, cuando corresponda, a partir del análisis y evaluación de los informes pertinentes.

5.3.2. - Entrenamiento y capacitación inicial

CODE100 S.A. realiza cursos de entrenamiento e instrucción en todas 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.

El personal de CODE100 S.A. es capacitado para poder cumplir con las funciones del rol asociado.

Los contenidos básicos se centrarán, entre otros, en los siguientes puntos relevantes:

Infraestructura de firma digital.

Responsabilidades y compromisos del rol y sus funciones.

Procedimientos y políticas operacionales y de seguridad relacionadas con la RA.

Uso y operaciones de hardware y software empleado en las RAs.

Manejo de incidentes y compromisos en materia de seguridad.

Procedimientos de recuperación ante desastres y manejo de la contingencia para la continuidad de actividades de la RA.

Gestión de la documentación inherente al funcionamiento de la RA.

Se llevará registro de los asistentes a la capacitación como de los resultados de la misma.

Se extenderán certificaciones de la capacitación.

5.3.3. - Frecuencia de procesos de actualización técnica

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.

El Jefe de Área comunicará al personal de CODE100 en forma periódica novedades en materia de tecnología de firma digital, en las implementaciones referidas a infraestructuras de clave pública o en materia de seguridad informática, si así lo requieren.

Evaluará en forma conjunta con los responsables de las otras áreas de CODE100 la factibilidad y beneficios de la implementación de novedades tecnológicas.

Asesorará a la máxima autoridad de CODE100 sobre los beneficios de los cambios propuestos.

5.3.4. - Frecuencia de rotación de cargos

No existe rotación entre los distintos cargos de la CA

Esto es extensivo a las RA.

5.3.5. - Sanciones a aplicar por acciones no autorizadas

Constatada la infracción o incumplimiento de la CP acordada y o cualquier otra vulneración a los compromisos asumidos por el personal que desempeña los roles que componen esta CA, se labrará el acta correspondiente, dejándose constancia de la fecha, hora y causa de la infracción y o incumplimiento.

Se comunicará el incumplimiento o infracción que se imputa, y se establecerá la sanción definitiva. Se notificará de modo fehaciente al acusado de la infracción. La sanción definitiva podrá ser la desvinculación de la persona de CODE100 S.A.

Durante el período de análisis del incumplimiento, la persona no podrá cumplir funciones en las áreas sensibles de la CA ni de la RA Central y le serán retiradas todas las autorizaciones de acceso físico y lógico.

Toda sanción a aplicar se comunicará a los interesados en un plazo no mayor a dos (2) días desde el momento de resolución de aplicación.

En caso de apreciarse mala fe en la utilización de los recursos informáticos de CODE100 S.A. -principalmente aplicaciones y/o datos– CODE100 S.A. ejercerá las acciones que legalmente le amparen para la protección de sus derechos y sus recursos informáticos.

a) En el caso de detectase una conducta susceptible de ser constitutiva de infracción quien lo detecte, lo comunicará inmediatamente al Coordinador de Seguridad.

b) En el plazo de tres días el Coordinador de Seguridad calificará la gravedad de la infracción y,

   - Si estimase que se trata de una falta leve acordará sin más trámite la imposición de la correspondiente sanción.
   - Si estimase que se trata de una **infracción grave o muy grave**, lo comunicará inmediatamente al Responsable de Firma Digital y Responsable de Recursos Humanos.

c) Tratándose de una infracción grave o muy grave el Responsable de Recursos Humanos instruirá el correspondiente expediente, del cual se dejará constancia por escrito, en el cual:

   - Oirá al Responsable que hubiera realizado la comunicación y en su caso, al trabajador afectado.
   - Resolverá, previo asesoramiento técnico oportuno, sobre si la conducta es o no sancionable, y, en el primer caso, procederá a determinar su gravedad atendiendo a:

     - El mayor o menor grado de responsabilidad del trabajador.

     - Su categoría profesional.

     - La repercusión que la conducta infractora tenga en la empresa.

   - Toda resolución que acuerde la imposición de una sanción deberá ser motivada, y en ella se explicitarán los datos del lugar donde ocurrió, del trabajador sancionado y una descripción completa de la infracción (lugar

fecha y hora, descripción de la conducta y circunstancias determinantes de su gravedad).

d) La notificación de la sanción se realizará siempre por medio fehaciente, que deje constancia tanto del hecho de la notificación, como de su contenido.

- Si se realiza de forma presencial, la copia de la notificación deberá ser firmada por el trabajador con expresión de la fecha en que se le efectúa la misma.
- En otro caso, se efectuará por medio de telegrama con acuse de recibo o medio similar. Se evitarán aquellos sistemas que no dejen constancia del contenido de la notificación.

e) Cuando se impusiere una sanción muy grave se informará a la Máxima Autoridad de CODE100 S.A.
f) La valoración de las faltas y las correspondientes sanciones impuestas por la dirección de la empresa serán siempre revisables ante la jurisdicción competente.

5.3.6. - Requisitos para contratación de personal

El personal a ser contratado a los efectos de cumplir acciones en servicio de certificación digital del PSC en el marco de su CP deberá tener el conocimiento y formación suficiente para el mejor cometido de las funciones asignadas. Para ello, CODE100 S.A. llevará a cabo los procesos de selección de personal y capacitación que estime necesarios con el objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

Proceso de Selección

ETAPA	ACTIVIDAD	RESPONSABLE
Convocatoria	Elaborar en forma conjunta con el Área solicitante (es decir, la que necesita cubrir cargos vacantes) la Convocatoria con la siguiente información: - Tipo de Convocatoria - Información del cargo (denominación, grado, código, remuneración, etc.) - Ubicación orgánica y jerárquica del Rol - Número de vacantes a cubrir - Requisitos mínimos exigidos - Rol y Funciones específicas	RRHH

	- Modalidad y fecha de inscripción - Lugar de realización del Proceso de Selección - Datos mínimos a consignar en el Curriculum Vitae - Prueba de Conocimientos y puntaje mínimo para la aprobación.	
	Publicar la Convocatoria en diario de circulación Provincial.	RRHH
	Recibir Hojas de Vida enviadas por los aspirantes en respuesta a la Convocatoria.	RRHH
Preselección de Aspirantes	Analizar y evaluar los datos consignados por los aspirantes en sus respectivos CVs y confrontarlos con los requisitos de las vacantes a cubrir.	RRHH
	Elaborar Lista de Aspirantes Preseleccionados	RRHH

5.3.7. - Documentación y materiales provistos al personal

Todo el personal involucrado en el funcionamiento de la CA es designado en sus funciones y comunicado de las tareas y procedimientos que debe cumplir.

Del mismo modo, si su función requiere de material adicional, como por ejemplo dispositivos criptográficos, cajas de seguridad, llaves, tarjetas de acceso, etc., éstos son entregados como paso previo a iniciar sus tareas.

Recursos Asignados:

Asignación de ecursos	Entregar al nuevo empleado la tarjeta de proximidad para acceso al edificio de CODE100 S.A.	RRHH
	Comunicar al nuevo empleado cuál es el puesto de trabajo dentro de CODE100 S.A.	RRHH
	Comunicar al nuevo empleado cuál es la computadora que utilizará para desempeñar sus tareas.	RRHH
Asignación de usuarios y contraseñas	Comunicar al nuevo empleado su identificación de usuario y su contraseña para que pueda llevar a cabo los accesos lógicos correspondientes a su rol y funciones.	Responsable de la CA
Capacitación del personal	Capacitar y entrenar al personal para el puesto de trabajo.	Responsable según corresponda

	Comunicar horarios laborales.	Responsable de RRHH
Asignación de documentación de CODE100	El personal de CODE100 S.A. es capacitado para poder cumplir con las funciones del rol asociado. Los contenidos básicos se centrarán, entre otros, en los siguientes puntos relevantes: Infraestructura de firma digital. Responsabilidades y compromisos del rol y sus funciones. Procedimientos y políticas operacionales y de seguridad relacionadas con la RA Uso y operaciones de hardware y software empleado. Manejo de incidentes y compromisos en materia de seguridad. Procedimientos de recuperación ante desastres y manejo de la contingencia para la continuidad de actividades. Gestión de la documentación.	Responsable de RRHH

El detalle del material adicional requerido por la RA figura en el documento "Guía de instalación y funcionamiento de las RA".

En conformidad con el material entregado, el personal firma un acuse de recibo y compromiso de confidencialidad en los casos correspondientes.

6. - CONTROLES DE SEGURIDAD TECNICA

6.1. - Generación e instalación del par de claves criptográficas

6.1.1. - Generación del par de claves criptográficas

Ver punto 6.1.1 Manual de Procedimientos de Certificación (Reservado)

6.1.2. - Entrega de la clave privada al suscriptor

Ver punto 6.1.1 Manual de Procedimientos de Certificación (Reservado)

6.1.3. - Entrega de la clave pública al emisor del certificado

Ver punto 6.1.1 Manual de Procedimientos de Certificación (Reservado)

6.1.4. - Disponibilidad de la clave pública del certificador

Ver punto 6.1.4 Manual de Procedimientos de Certificación (Reservado)

6.1.5. - Tamaño de claves

Ver punto 6.1.5 Manual de Procedimientos de Certificación (Reservado)

6.1.6. - Generación de parámetros de claves asimétricas

Ver punto 6.1.6 Manual de Procedimientos de Certificación (Reservado)

6.1.7. - Verificación de calidad de los parámetros

Ver punto 6.1.7 Manual de Procedimientos de Certificación (Reservado)

6.1.8. - Generación de claves por hardware

Ver punto 6.1.8 Manual de Procedimientos de Certificación (Reservado).

6.1.9. - Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v.3)

Ver punto 6.1.9 Manual de Procedimientos de Certificación (Reservado).

6.2. - Protección de la clave privada

La protección de la clave privada, considerada en este punto, se aplica para la CA, las RA y los suscriptores, según se detalla a continuación.

6.2.1. - Estándares para dispositivos criptográficos

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

Las claves privadas de las RA son generadas y almacenadas en un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 2.

La clave privada del suscriptor persona física es generada y almacenada por "hardware" sobre dispositivos criptográficos diseñados para tal fin que cumplen con las normas FIPS 140-2 nivel 2.

La clave privada del suscriptor persona jurídica es generada y almacenada por hardware sobre dispositivos criptográficos diseñados para tal fin que cumplen con las normas FIPS 140-2 nivel 3.

El dispositivo criptográfico 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.

6.2.2. - Control "M de N" de clave privada

La clave privada de la CA es activada exclusivamente en las instalaciones de CODE100 S.A. o en su sitio alternativo, dentro del nivel de seguridad asignado a las operaciones críticas de la CA. Para su activación deben estar presentes, por lo menos, el Responsable Técnico, el Coordinador de Seguridad y los oficiales habilitadores o testigos en un número 3 de 10 posibles.

Las RA y los suscriptores de certificados con dispositivos criptográficos de su propiedad tienen acceso a su clave privada personal a través de un PIN de acceso al dispositivo criptográfico y contraseña de la clave privada.

6.2.3. - Recuperación de clave privada

La especificación conceptual puede encontrarse en "4.12 – Custodia y recuperación de claves" de la CP.

Para el procedimiento de recuperación de la clave privada de la CA se debe disponer de la copia de seguridad ("backup") en un dispositivo PCMCIA. Se debe tener presente que tanto la obtención de la copia como la recuperación sólo pueden ser realizadas por personal autorizado sobre dispositivos criptográficos seguros, de los que dispone CODE100 S.A., y exclusivamente en los niveles de seguridad de la CA en su sitio principal o en su sitio alternativo.

El procedimiento en sí mismo es reservado, no es información de divulgación pública.

El resultado del procedimiento es la disponibilidad del servicio de certificación digital, en el sitio principal o en el de contingencia, según como se hubiera requerido.

No se implementan mecanismos de resguardo y recuperación de la clave privada de las RA, ni de los suscriptores. En caso de compromiso de la clave privada, éstos deberán proceder a la revocación del certificado y a la tramitación de una nueva solicitud de emisión de certificado, si asícorrespondiere.

6.2.4. - Copia de seguridad de clave privada

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

El procedimiento es reservado.

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

6.2.5. - Archivo de 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.

El procedimiento es reservado.

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

6.2.6. - Incorporación de claves privadas en dispositivos criptográficos

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

El procedimiento para la CA es reservado.

Las claves privadas de los Suscriptores personas físicas son generadas y almacenadas en esos dispositivos, que estarán homologados como FIPS 140-2 nivel 2 y no permiten su exportación.

Las claves privadas de los Suscriptores personas jurídicas son generadas y almacenadas en esos dispositivos, que estarán homologados como FIPS 140-2 nivel 3 y no permiten su exportación.

El procedimiento para los Suscriptores, descripto en "4.1. Solicitud de certificados".

6.2.7. - Método de activación de claves privadas

Para la activación de la clave privada de la CA deben estar presentes, por lo menos, el Responsable Técnico, el Coordinador de Seguridad y los oficiales habilitadores en número 3 de 10. Los responsables necesarios para la activación deberán identificarse frente al sistema según corresponda al rol asignado por medio de distintos mecanismo de autenticación, a saber: llave de seguridad, claves secretas o ambos.

El procedimiento es reservado.

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

6.2.8. - Método de desactivación de claves privadas

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, el que debe estar debidamente autorizado por el Responsable de Firma Digital, quien debe, además, participar en la Ceremonia de desactivación de la clave privada de la CA.

El procedimiento es reservado.

6.2.9. - Método de destrucción de claves privadas

Una vez finalizada la vida útil de la clave privada de la CA, con motivo de la revocación o expiración del certificado asociado, la partición del dispositivo criptográfico contenedor de esa clave privada será borrada y "formateada" según el documento Plan de Seguridad.

El procedimiento es reservado.

Para el caso de que finalice la vida útil de la clave privada de una RA o de un suscriptor, por motivo de revocación o expiración del certificado asociado, el correspondiente dispositivo criptográfico será inicializado nuevamente por su propietario.

6.3. - Otros aspectos de administración de claves

6.3.1. - Archivo permanente 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, lo cual, sumado a la firma 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.

El procedimiento para la toma de la copia de respaldo y para su restauración se ejecuta en forma periódica, de acuerdo con un programa establecido. Es requisito previo la disponibilidad de los medios de almacenamiento seguro para contener las copias.

El detalle del procedimiento no es de disponibilidad pública, sino reservada.

6.3.2. - Periodo de uso de clave pública y privada

El par de claves criptográficas del certificado de la CA tiene una validez de diez (10) años.

En el caso del PSC el tiempo de uso es de ocho (8) años y el tiempo operacional de diez (10) años.

El par de claves criptográficas correspondientes a los certificados emitidos por la CA podrán ser utilizadas por su suscriptor únicamente durante el periodo de validez de los certificados. Ese período será de máximo de dos (2) años para todos los certificados de persona física o jurídica, que es también su tiempo de uso.

6.4. - Datos de activación

6.4.1. - Generación e instalación de datos de activación

Los dispositivos criptográficos utilizados por la RA Central y los suscriptores que los tengan para la generación, almacenamiento y uso de la clave privada, son inicializados por ellos.

Como paso previo a la generación de la clave privada, las RA y los suscriptores que posean estos dispositivos, deberán establecer una clave de seguridad de acceso sobre el dispositivo criptográfico denominado PIN y al momento de la generación la contraseña de la clave privada. El PIN de acceso del dispositivo criptográfico y 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.

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.

Este procedimiento es reservado.

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 del PIN de acceso del dispositivo criptográfico y contraseña de la clave privada.

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

Este procedimiento es reservado.

6.4.3. - Otros aspectos referidos a los datos de activación

Es responsabilidad de las RA y de los suscriptores, elegir contraseñas para sus claves privadas y PIN 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.

El PIN de acceso del dispositivo criptográfico debe diferir de la contraseña de la clave privada.

6.5. - Controles de seguridad informática

6.5.1. - Requisitos Técnicos 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:

a) 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.

b) Separación de funciones y roles críticos

Las principales funciones vinculadas a los procesos de seguridad y 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 diferentes responsables. En caso de ausencia temporaria, el responsable será reemplazado por su correspondiente sustituto.

Esto aplica también a las RA . Para mayor detalle ver el documento "Guía de instalación y funcionamiento de las RA".

c) Identificación y autenticación de roles

Para la identificación y autenticación en cada uno de los roles con acceso al sitio de máxima seguridad:

Jefe de Área

Responsable Técnico

Coordinador de Seguridad

Responsable de Firma Digital

Oficial Criptográfico

Los cuales se encuentran 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.

d) Utilización de criptografía para las sesiones de comunicación.

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

e) Archivo de datos históricos y de auditoría del certificador 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.

f) 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.

g) Prueba de seguridad.

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

h) 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. - Calificaciones de seguridad computacional

Los servidores que conforman la CA se encuentran alojados en el Sitio de Máxima Seguridad o "SMS" construido con las certificaciones requeridas 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 CODE100DOC

El software PKI utilizado por la CA, se basa en todos los servicios de certificados nativos del 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: IETF: RFC5280 upd by 6818, CMC., CMC.

6.6. - Controles Técnicos del ciclo de vida de los sistemas

6.6.1. - Controles de desarrollo de sistemas

Los sistemas informáticos adquiridos 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 declarados por el proveedor y oportunamente aceptados cuando fueron seleccionados.

CODE100 S.A. ha adoptado el modelo de la organización OWASP (Open Web Application Security Project), como su estándar para la seguridad de los sistemas, que aplica tanto en los desarrollos que realiza como en la homologación del software adquirido y en las adaptaciones y el mantenimiento de aplicaciones, según su Política de Desarrollo de Software.

6.6.1.1. Descripción del modelo OWASP

El modelo elaborado por la organización OWASP se maneja con una lista de las 10 vulnerabilidades más frecuentes encontradas en las aplicaciones web, ordenadas según el número de casos. Esa lista es dinámica y se actualiza con una frecuencia anual para adaptarla a la realidad encontrada mediante encuestas y procesamiento estadístico. Este modelo incluye también la recomendación de procedimientos para detección de cada una de esas vulnerabilidades en las aplicaciones, tanto adquiridas en forma de paquete terminado como en las desarrolladas por la organización.

Más información puede encontrarse en: https://www.owasp.org/

6.6.1.2. Control de aplicaciones usando el modelo OWASP

El responsable de aplicaciones de CODE100 S.A. sigue los lineamientos de este modelo, con un grupo de profesionales entrenados. Su misión es certificar el cumplimiento del modelo por parte de cada aplicación antes de su implementación para el servicio de firma digital. Los controles son auditados en forma periódica según las especificaciones de la Política de Desarrollo de Software.

6.6.2. - Administración de controles y seguridad

CODE100 S.A. mantiene el control de los equipos por medio del inventario y de la documentación de la configuración del sistema, registrándose de inmediato toda modificación o actualización a cualquiera de ellos. Los controles son auditados en forma periódica según las especificaciones de la Política de Seguridad.

El esquema de seguridad física del Sitio de Máxima Seguridad donde se aloja la CA previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones.

El control periódico de integridad del sistema de la CA, realizado por el servicio CODE100MON, advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

6.6.3. - Calificaciones de seguridad del ciclo de vida del software

No existen certificaciones de terceros respecto del ciclo de vida del software.

6.7. - Controles de seguridad de red

CODE100 S.A. posee un sistema de protección integral de sus activos informáticos. La red de la CA se encuentra delimitada por "firewalls" que proveen el filtrado de los paquetes de datos.

6.8. - Controles de ingeniería de dispositivos criptográficos

Las actualizaciones de software o "firmware" de los dispositivos criptográficos utilizados por la CA son verificados en ambientes de prueba independientes y, en caso de ser aprobadas por el personal técnico de CODE100 S. A., son distribuidas y aplicadas en los sistemas correspondientes.

7. - PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

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".

Las listas de certificados revocados (CRLs) cumplen con los requerimientos de la Ley Nro. 4017/10, Nro. 4610/12, Decreto Reglamentario Nro. 7369/11 y las especificaciones contenidas en el RFC 5280.

7.1. - Perfil del certificado

El formato de los certificados digitales emitidos bajo esta política cumple con los requerimientos de la Infraestructura de Clave Pública del Paraguay y las especificaciones contenidas en RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile" y RFC 5280.

Bajo esta CP se emitirán 2 tipos de certificados: 1) Para Personas Físicas y 2) Para Personas Jurídicas

7.1.1. Perfil del certificado para persona física

La información detallada se encuentra en "7.1.1. Perfil del certificado para persona física" de la CP.

7.1.2. Perfil del certificado para persona jurídica

La información detallada se encuentra en "7.1.3. Perfil del certificado para persona jurídica" de la CP.

7.2. - Perfil de la lista de certificados revocados

La información detallada se encuentra en "7.2. - Perfil de la lista de certificados revocados" de la CP.

8. - ADMINISTRACION DE ESPECIFICACIONES

8.1. - Procedimientos de cambio de especificaciones

La CP y sus documentos relacionados serán revisados por CODE100 S. A. en forma periódica para detectar y corregir eventuales faltas de claridad y para adaptarlos a cambios en la normativa. Esos cambios no serán de magnitud tal que pueda afectar a los certificados vigentes y su posibilidad de uso para la que fue emitido.

Todo cambio será sometido a la aprobación de la AA y, una vez aprobado, publicado en el sitio web de CODE100 S.A. y puesto en vigencia.

Cada nueva versión tendrá una descripción de los cambios producidos referidos a la versión previa.

El Responsable de Firma Digital eleva las propuestas al Directorio de CODE100 S.A. sobre los cambios en las Políticas de Certificación, Manuales de Procedimientos y otros documentos de la CA.

El Directorio evalúa la viabilidad de los cambios a fin de ser aprobados por la autoridad de aplicación.

Una vez aprobados se realiza la actualización de los documentos con su correspondiente versionado.

El Responsable de Firma Digital notificará en forma fehaciente a la Autoridad de Aplicación de Firma Digital de la República del Paraguay los cambios propuestos para la documentación.

8.2. - Procedimientos de publicación y notificación

Una copia actualizada del presente documento se encuentra permanentemente disponible en forma pública y accesible a través de Internet en la dirección:

- http://www.CODE100.com.py/firma-digital

En caso de producirse modificaciones sustanciales a los contenidos de la CP o a alguno de los documentos relacionados, los suscriptores que posean certificados vigentes a la fecha de aplicación del cambio serán notificados por correo electrónico en las direcciones declaradas en los correspondientes certificados.

8.3. - Procedimientos de aprobación

Según lo establecido por la Ley 4.710 y por la Infraestructura de Clave Pública del Paraguay, la CP, la CPS y los documentos relacionados obligatorios, así como sus modificaciones, deben ser aprobados por el Ministerio Industria y Comercio (MIC), en su carácter de AA de la Infraestructura de Clave Pública del Paraguay.