Política de Certificación de la Autoridad Certificadora Raíz Nacional

Unidad de Certificación Electrónica

Infraestructura Nacional de Certificación Electrónica
República Oriental del Uruguay

Índice

1 - Introducción

1.1 - Descripción general

En el marco de la Infraestructura Nacional de Certificación Electrónica en Uruguay (PKI Uruguay, por sus siglas en inglés) funciona, como organismo acreditador y regulador, la Unidad de Certificación Electrónica (UCE).

La UCE cumple tres roles centrales en la operación de PKI Uruguay:

a) promueve y aprueba las Políticas de Certificación que indican los perfiles de certificados electrónicos y aplicabilidad a diversos grupos de interés;

b) acredita a Prestadores de Servicios de Certificación (PSC) a emitir certificados de acuerdo a estas Políticas; y,

c) audita la actividad de los PSC.

De acuerdo a lo estipulado en la Ley 18.600, la operación de la Autoridad Certificadora Raíz Nacional (ACRN) es realizada por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). La ACRN es la raíz de la cadena de confianza. Su certificado es autofirmado y aceptado expresamente por los Terceros que establecen confianza en la PKI Uruguay.

La AGESIC, a través de la ACRN, habilita tecnológicamente la operación de los Prestadores de Servicios de Certificación Acreditados (PSCA) emitiendo certificados electrónicos para sus Autoridades Certificadoras (ACPA – Autoridad Certificadora del Prestador Acreditado). De esta forma, las ACPA pasan a ser parte de la cadena de confianza de la PKI Uruguay.

Los certificados emitidos por la ACRN y dirigidos a las ACPA se rigen por la presente Política de Certificación y por la Declaración de Prácticas de Certificación de la ACRN. Por lo tanto, las ACPA y los Terceros aceptantes de dichos certificados cuentan con el respaldo de PKI Uruguay para las operaciones de firma electrónica que correspondan.

La validez de la firma electrónica en Uruguay y la designación de los órganos competentes para su operación se encuentran declaradas en la Ley 18.600:

Artículo 1º. (Ámbito de aplicación).- Queda reconocida la admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica.

Los servicios de certificación electrónica deberán ajustarse a lo previsto en esta ley, su actividad no estará sujeta a autorización previa[1] *y se realizará en régimen de libre competencia, sin que ello implique sustituir o modificar las normas que regulan las funciones que corresponde realizar a quienes están facultados legalmente para dar fe pública.*

Las disposiciones de esta ley no alteran el Derecho preexistente respecto a la celebración, perfeccionamiento, validez y eficacia de los actos y negocios jurídicos.

Artículo 6º. (Efectos legales de la firma electrónica avanzada).- La firma electrónica avanzada tendrá idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas, siempre que esté debidamente autenticada por claves u otros procedimientos seguros que:

a) garanticen que la firma electrónica avanzada se corresponde con el certificado reconocido emitido por un prestador de servicios de certificación acreditado, que lo asocia con la identificación del signatario;

b) aseguren que la firma electrónica avanzada se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado; y

c) garanticen que la firma electrónica avanzada ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado reconocido.

El documento electrónico suscripto con firma electrónica avanzada tendrá idéntico valor probatorio al documento público o al documento privado con firmas certificadas en soporte papel. El documento electrónico no hará fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador de servicios de certificación acreditado.

Artículo 14. (Competencia).- La Unidad de Certificación Electrónica deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de esta ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) De acreditación:

i. Recibir, tramitar y resolver las solicitudes de acreditación de los prestadores de servicios de certificación.

[1] Esto aplica a Autoridades Certificadoras de particulares. Los prestadores que operen bajo PKI Uruguay deberán estar previamente acreditados por la UCE.

ii. *Inscribir a los prestadores de servicios de certificación en el Registro de Prestadores de Servicios de Certificación Acreditados, que a tal efecto se crea en esta ley, una vez otorgada la acreditación.*

iii. *Suspender o revocar la inscripción de los prestadores de servicios de certificación acreditados.*

iv. *Mantener en el sitio web de la Unidad de Certificación Electrónica la información relativa al Registro de Prestadores de Servicios de Certificación Acreditados, tales como altas, bajas, sanciones y revocaciones.*

b) *De control:*

i. *Controlar la calidad y confiabilidad de los servicios brindados por los prestadores de servicios de certificación acreditados, así como los procedimientos de auditoría que se establezcan en la reglamentación.*

ii. *Realizar auditorías a los prestadores de servicios de certificación acreditados, de conformidad con los criterios que la reglamentación establezca para verificar todos los aspectos relacionados con el ciclo de vida de los certificados reconocidos y de sus claves criptográficas.*

iii. *Determinar las medidas que estime necesarias para proteger la confidencialidad de los titulares de certificados reconocidos.*

iv. *Efectuar inspecciones y requerir en cualquier momento a los prestadores de servicios de certificación acreditados toda la información necesaria para garantizar el cumplimiento de la función en los términos definidos en esta ley y su reglamento.*

c) *De instrucción:*

i. *Recibir y evaluar reclamos de titulares de certificados reconocidos relativos a la prestación de servicios de certificación, sin perjuicio de la responsabilidad directa que el prestador de servicios de certificación acreditado tiene ante el titular.*

d) *De regulación:*

i. *Definir los estándares técnicos y operativos que deberán cumplir los prestadores de servicios de certificación acreditados, así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.*

ii. *Fijar reglas y patrones industriales que aseguren la compatibilidad, interconexión e interoperabilidad, así como el correcto y seguro funcionamiento de los dispositivos de creación y verificación de firma, controlando su aplicación.*

e) *De sanción:*

i. *La Unidad de Certificación Electrónica podrá imponer al prestador de servicios de certificación acreditado que infringiere total o parcialmente cualesquiera de las obligaciones derivadas de esta ley o de las normas que resulten aplicables al servicio que presta, las sanciones que se graduarán en atención a la gravedad o reiteración de la infracción, que se detallan a continuación:*

i. *Apercibimiento.*

ii. *Multa entre 100.000 UI (cien mil unidades indexadas) y 4.000.000 UI (cuatro millones de unidades indexadas).*

iii. *Suspensión hasta por un año de la acreditación.*

iv. *Revocación de la acreditación.*

ii. *Las sanciones podrán aplicarse independiente o conjuntamente, según resulte de las circunstancias del caso.*

iii. *Las resoluciones que impongan sanciones pecuniarias de acuerdo a lo previsto en esta ley, constituyen título ejecutivo a todos sus efectos.*

Artículo 15. (Autoridad Certificadora Raíz Nacional).- La Autoridad Certificadora Raíz Nacional es la primera autoridad de la cadena de certificación a la cual le compete emitir, distribuir, revocar y administrar los certificados de los prestadores de servicios de certificación acreditados.

Desígnase a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento como Autoridad Certificadora Raíz Nacional.

La presente Política de Certificación de la ACRN describe los certificados emitidos por la misma que habilitan la operación de las ACPA.

1.2 - Identificación de la Política de Certificación

Nombre: Política de Certificación de la ACRN

Versión: 1.1

Fecha de elaboración: 05/10/2011

Fecha de última actualización: 17/04/2013

OID: 2.16.858.10000157.66565.0

Sitio web de publicación: www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf

1.3 - Participantes de la PKI Uruguay

1.3.1 – Unidad Reguladora

El rol de Ente regulador incluye la totalidad de funciones relativas a la definición de las normas que regulan el funcionamiento de los diferentes actores de la Infraestructura Nacional de Certificación Electrónica. De acuerdo a la Ley 18.600 ese rol es desempeñado por la UCE.

1.3.1.1 - UCE

Como unidad reguladora, la UCE desempeña las siguientes funciones:

a) Definir y aprobar las Políticas de Certificación que definen los perfiles de certificados de la PKI Uruguay;

b) Desarrollar el proceso de acreditación de Prestadores, autorizando o denegando la operación de los mismos dentro de la PKI Uruguay;

c) Solicitar a la Unidad Nacional de Asignación de OID (UNAOID), en su rol de Administrador de la rama de OIDs de Uruguay, un OID para cada Política de Certificación aprobada;

d) Publicar y mantener actualizada la Lista de Prestadores de Servicios de Certificación Acreditados y Suspendidos, incluyendo la información pública de

contacto de cada uno de ellos y las Políticas de Certificación para las cuales están acreditados a emitir certificados;

e) Realizar auditorías periódicas a los PSCA para verificar el cumplimiento con las normativas legales vigentes y las Políticas de Certificación para las cuales emiten certificados

1.3.2 - Autoridades de certificación

El rol de Autoridad de Certificación incluye las funciones relativas a la gestión de certificados electrónicos que habiliten o inhabiliten tecnológicamente la operación de los Prestadores de Servicios de Certificación Acreditados, según lo dispuesto por la presente Política de Certificación y la normativa legal vigente. El rol de Autoridad de Certificación para la ACRN es cumplido por la AGESIC según lo estipulado por la Ley 18.600. La Autoridad de Certificación responde a las solicitudes del Suscriptor de los certificados a través de su Autoridad de Registro (ver 1.3.3 – Autoridad de Registro).

Como autoridad de certificación, la ACRN desempeña las siguientes funciones:

a) Emitir, Renovar y Revocar el certificado público de la ACRN;

b) A solicitud de la UCE, Emitir, Renovar y Revocar certificados que habilitan la operación de los PSCA;

c) Publicar y mantener actualizada la Lista de Certificados Revocados (CRL, por sus siglas en inglés) para todos los certificados emitidos que apliquen a la presente Política;

d) Publicar documentación de la ACRN y aplicable a ella, como la presente Política de Certificación, la Declaración de Prácticas de Certificación de la ACRN y el Acuerdo con los PSC;

e) Publicar los certificados emitidos a los PSCA.

1.3.3 - Autoridad de Registro

La Autoridad de Registro cumple la función de procesar los requerimientos de los Suscriptores relativos a la emisión, renovación y revocación de certificados emitidos por la Autoridad de Certificación.

Las funciones de Autoridad de Registro para la ACRN son desempeñadas por la AGESIC.

Como Autoridad de Registro, la ACRN desempeña las siguientes funciones:

a) Iniciar el proceso de emisión de certificados de la ACRN para las ACPA, de acuerdo a lo establecido en el punto 4.1 de la presente Política;

b) Iniciar el proceso de revocación de los certificados emitidos por la ACRN, de acuerdo a lo establecido en el punto 4.9 de la presente Política;

c) Iniciar el proceso de renovación de certificados emitidos por la ACRN, de acuerdo a lo establecido en el punto 4.6 de la presente Política;

1.3.4 - Suscriptores

Los suscriptores de los certificados emitidos por la ACRN son los PSCA.

1.3.4.1 - Prestadores de Servicios de Certificación Acreditados

Los PSCA realizan las siguientes funciones:

a) Publicar y mantener actualizada su Declaración de Prácticas de Certificación (CPS, por sus siglas en inglés);

b) Mantener la infraestructura necesaria para la operación de su Autoridad Certificadora en las condiciones de seguridad requeridas por la presente Política, por la Declaración de Prácticas de Certificación, por las Políticas de Certificación para las cuales emite certificados y demás normativa vigente aplicable;

c) Emitir, renovar y revocar certificados electrónicos a suscriptores y usuarios finales de acuerdo a su Declaración de Prácticas de Certificación y a la Política de Certificación que aplique;

d) Mantener y actualizar el repositorio público de información;

e) Realizar funciones de Autoridad de Registro para los certificados que emite.

1.3.5 – Terceros aceptantes

Los Terceros aceptantes son las entidades o personas que confían en los certificados emitidos por la ACRN a los PSCA bajo la presente Política. Los Terceros aceptantes utilizan estos certificados para validar la cadena de confianza de la PKI.

1.4 - Uso de los certificados

Los certificados emitidos por la ACRN bajo la presente Política de Certificación pueden ser utilizados por los PSCA con el único propósito de validar la cadena de confianza de la PKI, firmar los certificados emitidos a sus suscriptores finales y firmar las Listas de Revocación de Certificados correspondientes.

Los certificados no pueden ser utilizados con otro fin. La utilización de la llave privada asociada al certificado para otro fin es considerada causal de revocación del mismo (ver 4.9.1)

1.5 - Administración de la Política

La Administración de la presente Política de Certificación es responsabilidad de la UCE.

Por consultas o sugerencias, la UCE designa al siguiente contacto:

Nombre: Unidad de Certificación Electrónica

Dirección de correo: infouce@uce.gub.uy

Teléfono: (+598) 2901 2929

1.6 - Relación entre la Política de Certificación y otros documentos

Este documento contiene la Política de Certificación de la Unidad de Certificación Electrónica (UCE). Una Política de Certificación es un conjunto de principios y reglas relativas a la emisión y gestión de certificados electrónicos, con soporte de claves públicas, que pueden utilizarse en diferentes servicios, como la autenticación de la identidad, la integridad y la autenticidad documental o el secreto de los datos, documentos y transmisiones.

La Política de Certificación establece las reglas mínimas que se deben cumplir por parte de los Prestadores de Servicios de Certificación Acreditados (PSCA) y los terceros aceptantes de certificados.

Por otra parte, todo Prestador de Servicios de Certificación debe disponer de una Declaración de Prácticas de Certificación con los procedimientos que aplica en la prestación de sus servicios, en cumplimiento con lo establecido en la Ley No 18.600, indicando el grado de aplicación de los requisitos establecidos por las Políticas de Certificación que gestiona detallando sus prácticas profesionales en relación con la provisión de los servicios de certificación.

Esta documentación se relaciona con la documentación auxiliar, entre la que se deben encontrar los instrumentos jurídicos reguladores de la prestación de servicios (documentación jurídica auxiliar), documentación de seguridad, documentación de operación y documentación de archivo.

1.7 - Procedimiento de Aprobación

El sistema documental y de organización de la UCE tendrá que garantizar, a través de la existencia y de la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la Política de Certificación y de las especificaciones del servicio relacionadas con ella. Se prevén, de esta forma, el procedimiento de modificación de especificación del servicio y el procedimiento de publicación de especificaciones del servicio. Las modificaciones finales de la Política de Certificación tendrán que ser aprobadas por la UCE, después de comprobar el cumplimiento de los requisitos establecidos en las secciones correspondiente de esta política.

1.8 - Definiciones y abreviaturas

Autoridad Certificadora Raíz Nacional (ACRN): conjunto de sistemas informáticos, personal, políticas y procedimientos que, en la estructura de PKI Uruguay por herencia, constituyen la raíz de confianza. Permite certificar a otras entidades encargadas de emitir certificados dentro de PKI Uruguay.

Prestador de Servicios de Certificación Acreditado (PSCA): entidad acreditada ante la UCE y responsable de la operación de una Autoridad de Certificación de PKI Uruguay.

Autoridad Certificadora del Prestador Acreditado (ACPA): suscriptor de los certificados emitidos por la ACRN que, durante su operativa, emite certificados a usuarios finales bajo las políticas de certificación que le fueron asignadas.

Terceros aceptantes: en el contexto de PKI Uruguay, usuarios que validan y confían en certificados emitidos por una Autoridad de Certificación de la PKI, sea la ACRN o una de las ACPA.

Política de Certificación (CP – Certificate Policy): conjunto de políticas que indican la aplicabilidad de un certificado a una comunidad particular y/o clase de solicitud con requerimientos comunes de seguridad, y además definen los requisitos que cualquier prestador debe respetar para trabajar con ese tipo de certificado. En el contexto de PKI Uruguay estas políticas son promovidas, aprobadas y mantenidas por la UCE.

Declaración de Prácticas de Certificación (CPS – Certificate Practice Statement): declaración de las prácticas que emplea una entidad certificadora en la gestión de los certificados emitidos por ella (emisión, revocación, renovación, etc.).

Solicitud de Firma de Certificado (CSR – Certificate Signing Request): es un mensaje emitido por la ACPA bajo el estándar PKCS#10 mediante el que solicita y provee información a la ACRN para la emisión de un certificado firmado por ella.

Escrow: acuerdo mediante el cual una clave privada puede ser custodiada por una entidad y, bajo ciertas circunstancias, ser devuelta a su legítimo dueño.

FIPS (Federal Information Processing Standard) 140 nivel 3: estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos. En su nivel 3 asegura que los módulos sean resistentes a la intrusión física.

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

2. – Aspectos Generales de la Política de Certificación

2.1. - Obligaciones

2.1.1. – Obligaciones de la Unidad Reguladora

2.1.1.1. - Obligaciones de la UCE

Constituyen obligaciones de la UCE en relación con la presente política:

a) La elaboración o aprobación, actualización y cancelación de las políticas de certificación de la PKI Uruguay;

b) La acreditación de los PSC para operar dentro de la PKI Uruguay;

c) La publicación de la lista de PSC Acreditados a operar en PKI Uruguay;

d) El control y auditoría de los PSCA para garantizar que sus prácticas cumplen con las políticas de certificación para las cuales fueron acreditados, la presente Política de Certificación, su Declaración de Prácticas de Certificación y la normativa legal vigente;

e) La publicación en el Sitio Oficial, y referencia en el Diario Oficial, de:

   i. La Resolución que ordena el otorgamiento, denegación, renovación, suspensión y/o revocación de acreditación para un PSC, y

   ii. El certificado electrónico emitido por la ACRN a la ACPA bajo la presente Política;

   iii. La modificación de la presente Política de Certificación.

f) Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad o confidencialidad según corresponda);

g) Mantener a disposición permanente del público las políticas de certificación de la PKI Uruguay;

h) Disponer de un servicio de atención que permita responder las consultas de los suscriptores de certificados emitidos por los PSCA y los Terceros aceptantes de dichos certificados;

i) Atender los requerimientos de revocación de certificados solicitados por los PSCA o por una autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;

j) Atender los requerimientos de suspensión de un PSCA por parte de una autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;

k) La publicación de la Lista de PSCA Suspendidos en su repositorio de información;

l) Notificar a los PSCA, como suscriptores de los certificados emitidos por la ACRN bajo la presente política, acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACRN y la emisión de un nuevo par de claves criptográficas, como también del procedimiento a seguir en ese caso;

m) Desarrollar, mantener y actualizar procedimientos que permitan la realización de sus actividades en cumplimiento con la presente Política de Certificación y la normativa legal vigente.

2.1.2. - Obligaciones del certificador

2.1.2.1. - Obligaciones de la ACRN

Constituyen obligaciones de la ACRN:

a) Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, en conformidad con lo pautado en la presente Política;

b) Notificar a la UCE ante cualquier operación;

c) Generar su clave privada con aprobación de la UCE y según lo pautado en el Guión de Ceremonia de Claves;

d) Proteger su clave privada;

e) Emitir y renovar su propio certificado con aprobación de la UCE y según lo pautado en el Guión de Ceremonia de Claves;

f) Revocar su propio certificado ante sospecha real de compromiso de la clave privada asociada;

g) Atender los requerimientos de revocación de certificados solicitados por los PSCA o por la UCE, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;

h) Utilizar el certificado de la ACRN de acuerdo con los requerimientos de la presente política de certificación;

i) La emisión, revocación y renovación de los certificados de las ACPA;

j) La emisión y publicación de su Lista de Certificados Revocados (CRL);

k) El envío a la UCE de las CRL inmediatamente después de emitidas;

l) Notificar a los PSCA, como suscriptores de los certificados emitidos por la ACRN bajo la presente política, acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACRN y la emisión de un nuevo par de claves criptográficas, como también del procedimiento a seguir en ese caso;

m) Garantizar el acceso permanente y gratuito de los suscriptores y Terceros aceptantes al sitio de publicación que contiene su propio certificado, los certificados emitidos a los PSCA y la lista de certificados revocados;

n) Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad o confidencialidad según corresponda).

2.1.3. - Obligaciones de la Autoridad de Registro de la ACRN

Las obligaciones de Autoridad de Registro de la ACRN son asumidas por la AGESIC:

a) Comprobar la validez de la acreditación para los PSCA que solicitan la emisión, revocación o renovación de un certificado;

b) Procesar las solicitudes de emisión, renovación o revocación de certificados emitidos por la ACRN;

c) Notificar a los PSCA ante la ocurrencia de un evento que así lo requiera según lo estipulado por la presente Política de Certificación;

d) Mantener un repositorio público de información de acuerdo al requerimiento 2.1.6 – Obligaciones del servicio de repositorio de la PKI Uruguay de la presente Política de Certificación.

El proceso de Acreditación de un Prestador de Servicios de Certificación se encuentra descripto en el documento "Procedimiento para la acreditación como Prestador de Servicios de Certificación de PKI Uruguay", publicado por la UCE en su sitio web (www.uce.gub.uy/informacion-tecnica/prestadores)

2.1.4. - Obligaciones de los Prestadores de Servicios de Certificación Acreditados

Los PSCA son personas físicas o jurídicas, públicas o privadas, nacionales o extranjeras, que expiden certificados electrónicos reconocidos u otros servicios en el marco de PKI Uruguay, bajo cuya responsabilidad recaerán las obligaciones citadas en este punto.

Toda la información necesaria para la identificación y autenticación del PSC a acreditar contenida en una solicitud de acreditación debe ser provista de forma completa y precisa al iniciar el proceso de acreditación. Dicha información se encuentra disponible en el Procedimiento para la acreditación como Prestador de Servicios de Certificación de PKI Uruguay, en www.uce.gub.uy/informacion-tecnica/prestadores.

Al aceptar un certificado emitido por la ACRN para su ACPA, el PSCA es responsable de toda la información por él provista y contenida en ese certificado.

La ACPA asociada al certificado emitido por la ACRN debe operar de acuerdo con su propia Declaración de Prácticas de Certificación (CPS), previamente aprobada por la UCE, y a las Políticas de Certificación de PKI Uruguay para las cuales se acreditó ante la UCE.

Los PSCA asumen las siguientes obligaciones:

a) Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, en conformidad con lo pautado en la presente Política y demás normativa vigente aplicable;

b) Proveer toda la información que le sea requerida de modo completo y preciso a fines de obtener el certificado emitido por la ACRN para su ACPA bajo la presente política de certificación;

c) Generar la clave privada de su ACPA en la condiciones establecidas en el punto 6.2.2;

d) Proteger la clave privada de su ACPA;

e) Solicitar la inmediata revocación del certificado emitido por la ACRN en el caso de compromiso o sospecha de compromiso de la clave privada de su ACPA;

f) Utilizar el certificado de su ACPA de acuerdo con los requerimientos de la presente política de certificación;

g) Mantener un sitio web donde publique de forma actualizada la información de acreditación ante la UCE, el certificado emitido por la ACRN a su ACPA y la información requerida por las políticas de certificación para las que se haya acreditado ante la UCE;

h) Publicar en dicho sitio web la Lista de Revocación de Certificados (CRL, por sus siglas en inglés) para los certificados que emita, de acuerdo a la reglamentación vigente;

i) Enviar diariamente la Lista de Revocación de Certificados a la UCE, en concordancia con la normativa vigente;

j) Cumplir con las obligaciones establecidas en la presente política de certificación, las políticas de certificación para las cuales se acredita y otros documentos aplicables emitidos por la UCE;

k) Firmar el Acuerdo con Suscriptores de Certificados de la ACRN, al aceptar el certificado emitido por la ACRN.

2.1.5. - Obligaciones de los Terceros aceptantes

Los Terceros aceptantes tienen las siguientes obligaciones:

a) Tomar conocimiento y aceptar los términos definidos en el presente documento, incluyendo y sin limitarse a:

   i. garantías y usos aceptables del certificado de la ACRN;

   ii. garantías y usos aceptables de los certificados emitidos por la ACRN a las ACPA;

   iii. obligaciones de los Terceros aceptantes

b) Tomar conocimiento y aceptar los términos definidos en la política de certificación bajo la cual el PSCA le emitió el certificado al suscriptor final;

c) Verificar la validez del certificado de la ACRN. El certificado de la ACRN es considerado válido cuando:

   i. Se encuentra dentro de su período de vigencia,

   ii. Su firma electrónica avanzada puede ser verificada con el uso del mismo certificado de la ACRN, y

   iii. No ha sido revocado según la CRL publicada por la ACRN.

d) Verificar la validez de los certificados emitidos por la ACRN a las ACPA. El certificado es considerado válido cuando;

   i. Se encuentra dentro de su período de vigencia,

   ii. Su firma electrónica puede ser verificada con la clave pública del certificado de la ACRN, y

   iii. No ha sido revocado según la CRL publicada por la ACRN.

e) Verificar que el certificado emitido por el PSCA sea utilizado para los propósitos previstos en esta política de certificación;

Las verificaciones requeridas en los puntos anteriores deben ser realizadas cada vez que el tercero confíe en un certificado emitido por un PSCA a un suscriptor final.

2.1.6. - Obligaciones del servicio de repositorio de la PKI Uruguay

Para esta política de certificación es obligación de la UCE el mantenimiento de un repositorio público de información, a través de un sitio web, que contenga la siguiente información:

a) Esta Política de Certificación (versión vigente y anteriores);

b) Todas las políticas de certificación que regulan la PKI Uruguay (versiones vigentes y anteriores);

c) Los requerimientos para la acreditación de un PSC;

d) Los requerimientos para la presentación de una nueva Política de Certificación, o modificación de una existente;

e) Las resoluciones mediante las que se acredita, suspende, renueva, revoca o deniega la acreditación a los PSC, con las razones pertinentes en el caso de suspensiones o revocaciones;

f) La lista de OIDs de políticas de certificación de la UCE bajo las que emiten certificados las ACPA, detallando qué OIDS está autorizada a utilizar en los certificados emitidos cada ACPA;

g) La lista de OIDs de la Declaración de Prácticas de Certificación de los PSCA;

h) Las listas de Certificados Revocados (CRL) de los PSCA, incluyendo la de la ACRN;

i) Información relevante de los informes de auditoría de la que fue objeto la UCE, la ACRN y los PSCA;

j) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto de la UCE;

k) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto de la ACRN;

l) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos designados por los PSCA para la atención a suscriptores finales y Terceros aceptantes;

m) Identificación, domicilio, números telefónico y dirección de correo electrónico de los PSC cuya acreditación haya sido revocada o expirado;

n) Leyes, Decretos y demás documentos regulatorios que afecten a la PKI Uruguay.

Para esta política de certificación es obligación de la ACRN el mantenimiento de un repositorio público de información, a través de un sitio web, que contenga la siguiente información:

a) Todas las políticas de certificación (versiones vigentes y anteriores) que utilice la ACRN para la emisión de certificados, incluyendo esta;

b) La Declaración de Prácticas de Certificación de la ACRN (versión vigente y anteriores);

c) El Acuerdo con Suscriptores de Certificados de la ACRN;

d) El certificado autofirmado de la ACRN;

e) Los certificados emitidos por la ACRN a las ACPA;

f) La Lista de Certificados Revocados (CRL) de la ACRN;

g) Referencia al sitio de publicación de información de la UCE;

h) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto de la ACRN.

2.2. - Responsabilidades

En relación con la responsabilidad, será de aplicación lo establecido en los artículos 24 y 25 de la Constitución de la República.

2.3. - Interpretación y aplicación de las normas

2.3.1. - Legislación aplicable

La interpretación, obligatoriedad, estructura y validez de esta Política de Certificación se encuentran regidas por la Ley No 18.600 y demás normas aplicables.

2.3.2. - Forma de interpretación y aplicación

Las disposiciones que surgen de la presente Política de Certificación son de cumplimiento obligatorio.

2.3.3. - Procedimientos de resolución de conflictos

Los PSCA en su calidad de suscriptores de certificados emitidos por la ACRN y los Terceros aceptantes de dichos certificados podrán interponer un recurso administrativo ante la UCE por conflictos referidos a la prestación del servicio.

2.4. - Publicación y Repositorios de certificados y listas de certificados revocados (CRLs)

2.4.1. - Publicación de información del certificador

En su rol de Unidad Reguladora, la UCE dispone del siguiente sitio web como repositorio público de información:

- www.uce.gub.uy

La ACRN, en su rol de Autoridad Certificadora, deberá disponer de un sitio de publicación de información, cuya URL se deberá especificar en la Declaración de Prácticas de Certificación de la ACRN.

La información mínima que la UCE y la ACRN deben publicar en los sitios webs se encuentra detallada en la sección 2.1.5 Obligaciones del servicio de repositorio de la PKI Uruguay.

2.4.2. - Frecuencia de publicación

La publicación o actualización de la información contenida en el repositorio público deberá contar con la verificación y aprobación de la UCE o de la ACRN según corresponda.

La información sobre políticas de certificación, acuerdos de privacidad y otros documentos relacionados será actualizada con un máximo de un (1) día hábil desde que se aprueben cambios.

La información relativa a datos de contacto será actualizada con un máximo de un (1) día hábil desde que se constaten cambios.

La información relativa al estado de la acreditación de los PSC será actualizada con un máximo de un (1) día hábil desde que se produzcan cambios.

La Lista de Certificados Revocados (CRL) de la ACRN deberá ser actualizada cuando ocurra al menos uno de los siguientes hechos:

a) se produzca la revocación de un certificado;

b) transcurran tres (3) meses desde la última emisión de la CRL

2.4.3. - Controles de acceso a la información

La UCE brinda acceso irrestricto a toda la información contenida en el repositorio público (ver 2.1.6), y establece controles adecuados para restringir la posibilidad de escritura y modificación de la información publicada, garantizando su integridad.

2.4.4. - Repositorios de certificados y listas de revocación

Los repositorios públicos de información de la UCE están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la UCE, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

La ACRN deberá garantizar niveles de servicio análogos para su servicio de publicación de información.

2.5. - Auditorías

La UCE se encuentra sujeta a auditorias periódicas. La información relevante de los informes de las auditorías es publicada en el sitio web de publicación de la UCE.

La ACRN se encuentra sometida a auditorías de la UCE. La información relevante de los informes de las auditorías es publicada en el sitio web de publicación de la UCE y deberá ser publicada en el sitio de publicación de la ACRN.

2.6. – Confidencialidad

A los efectos de la determinación del carácter de confidencial de la información recibida por la UCE se estará a los recaudos previstos de acuerdo con lo establecido en la Ley Nº 18.381, de 17 de octubre de 2008.

La información personal queda regulada por las Leyes Nos. 18.331, de 8 de agosto de 2008 y 18.381, de 17 de octubre de 2008.

2.6.1. – Publicación de información sobre los PSCA

La siguiente información referida a los PSCA se hará pública por parte de la UCE:

a) Los datos de contacto de los PSCA;

b) La información sobre el resultado de la auditoría de los PSCA;

c) Las políticas de certificación para las que se solicite aprobación por parte de la UCE;

d) Los requerimientos para la acreditación de los PSC;

e) Las resoluciones mediante las que se acredita, suspende, renueva, revoca o deniega la acreditación a los PSC.

2.6.2. - Publicación de información sobre la revocación o suspensión de un certificado

La información referida a la revocación de un certificado no se considera confidencial y deberá ser publicada por la ACRN a través de su CRL, publicada en el sitio www.agesic.gub.uy/acrn (la URL concreta deberá estar especificada en la CPS de la ACRN). Las razones que dan lugar a una revocación se consideran públicas, y estarán incluidas en el repositorio público de la UCE (www.uce.gub.uy/informacion-tecnica/prestadores).

La información sobre el estado de suspensión de un PSCA no se considera confidencial y se publica en el repositorio público de la UCE: www.uce.gub.uy/informacion-tecnica/prestadores. De la misma forma, las razones que dan lugar a la suspensión estarán incluidas en el repositorio público de la UCE, en la misma URL.

2.6.3. - Divulgación de información a autoridades judiciales

La condición de información secreta por ley, reservada o confidencial cesa ante la solicitud de juez competente en el marco de un proceso jurisdiccional.

2.6.4. - Divulgación de información por solicitud del suscriptor

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

2.6.5. - Otras circunstancias de divulgación de información

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

2.7. - Derechos de Propiedad Intelectual

La UCE mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la documentación y a publicaciones pertenecientes a ella. El documento podrá reproducirse o distribuirse atribuyendo su autoría a la UCE en forma precisa, completa y sin modificaciones.

3 - Identificación y Autenticación

3.1 – Registro Inicial

El PSCA podrá solicitar la emisión de los certificados ante la Autoridad de Registro de la ACRN. Dichos certificados serán emitidos bajo la presente Política de Certificación. El PSC deberá demostrar ante la ACRN una resolución de acreditación vigente ante la UCE para cada emisión de certificado que solicite.

Los certificados emitidos por la ACRN bajo la presente Política de Certificación habilitan tecnológicamente la operación de las ACPA como Autoridades de Certificación subordinadas de la ACRN dentro de la cadena de confianza de la PKI Uruguay. Las ACPA del PSCA, en caso de que operara más de una, se ubican al mismo nivel dentro de la cadena de confianza. No se permite en el contexto de PKI Uruguay la existencia de una ACPA subordinada a otra ACPA.

3.1.1 - Nominación

El nombre de la ACPA debe ser elegido por el PSCA.

El nombre elegido debe ser distintivo y estar asociado semánticamente al nombre legal del PSCA. Por ejemplo, si el nombre legal del PSCA fuera “Prestador ABC”, un nombre apropiado sería “Autoridad Certificadora del Prestador ABC”.

Los nombres elegidos deben ser únicos en el ámbito de la ACRN, de forma de identificar inequívocamente a cada PSCA.

En caso de que el PSCA opere más de una ACPA, los nombres para cada ACPA deben ser distintos.

La Autoridad de Registro de la ACRN asignará a la ACPA el nombre que figure en la resolución de acreditación correspondiente. Es responsabilidad de la UCE la aprobación de dicho nombre durante la acreditación.

3.1.1.1 – Formato del Nombre Distinguido

Para el nombre de la ACPA se deberá utilizar el campo “Subject” del certificado emitido por la ACRN (ver 7.2 Perfil del Certificado de las ACPA). El formato para indicar el nombre de la ACPA deberá ser X.500 (Distinguished Name).

Dicho formato, se aplicará de la siguiente forma:

Country: País del Prestador (UY)
Organization: Nombre legal o de fantasía del prestador.
Common Name: Nombre de la Autoridad Certificadora del Prestador.

Por mayor detalle acerca de la nominación y formatos de los nombres, referir al Punto 7 – Perfiles de Certificados y de Listas de Certificados Revocados.

A modo de ejemplo, el "Prestador ABC" podrá elegir su nombre distinguido de la siguiente manera:

C=UY
O=ABC
CN=Autoridad Certificadora de ABC

3.1.2 - Validación Inicial de Identidad

La Autoridad de Registro de la ACRN debe validar la identidad del solicitante previo a la emisión del certificado, como se estipula a continuación.

3.1.2.1 - Acreditación

a) Previo al proceso de registro, el PSC debe acreditarse ante la UCE para poder operar en el contexto de PKI Uruguay. Los requerimientos para la acreditación se encuentran en el Procedimiento para la acreditación como Prestador de Servicios de Certificación de PKI Uruguay, disponible en www.uce.gub.uy/informacion-tecnica/prestadores.

b) El PSCA debe demostrar ante la Autoridad de Registro de la ACRN la acreditación vigente ante la UCE.

3.1.2.2 - Identidad

La persona física designada por el PSCA para tramitar la emisión de un certificado, además de presentar la resolución de acreditación ante la UCE, deberá demostrar ante la Autoridad de Registro de la ACRN su identidad, presentando el documento de identificación correspondiente.

La ACRN deberá verificar que dichos datos además coincidan con los establecidos en la resolución de acreditación, la cual contendrá el nombre y número de documento de las personas autorizadas a solicitar el certificado.

3.1.2.3 - Clave privada

Para la emisión del certificado bajo la presente Política de Certificación, la ACRN debe validar que la llave privada correspondiente a la llave pública del CSR (Certificate Signing Request), emitido por una ACPA, este en posesión del PSCA y sea la misma utilizada para firmarlo. Para garantizar esto, un funcionario designado por la UCE y uno designado por la ACRN deberán estar presentes en el acto de generación de las llaves de la ACPA y firmar su conformidad con el proceso (ver 4.1 y 6.1.2). En ningún caso el PSCA se encuentra autorizado a compartir la llave privada de su/s ACPA con la ACRN (ver 4.1 Solicitud de Certificado).

Para el caso en que un PSCA opere más de una ACPA, los certificados y las llaves privadas asociadas deben ser únicos por ACPA.

3.1.3 - Identificación y Autenticación para Solicitudes de Cambio de Clave

No está permitido el cambio de claves de las ACPA ni de la ACRN como proceso independiente. Puede realizarse un cambio de clave en el marco de los procesos de renovación o revocación y reemisión de certificados.

3.1.4 - Identificación y Autenticación para Solicitudes de Revocación

La Autoridad de Registro de la ACRN debe validar la identidad del solicitante previamente a la solicitud de revocación del certificado emitido a una ACPA del PSCA. Para ello, el solicitante deberá estar habilitado por la UCE para solicitar la revocación y deberá identificarse oportunamente al igual que en el punto 3.1.2.2.

4 - Requerimientos Operativos del Ciclo de Vida de los Certificados

Los siguientes requerimientos están dirigidos a la ACRN, en su rol de Autoridad de Certificación Raíz, y a los PSCA en su rol de Suscriptores de los certificados emitidos bajo la presente Política. El objetivo es permitir una gestión segura del Ciclo de Vida de los Certificados emitidos por la ACRN.

4.1 - Solicitud de Certificado

El PSCA solicita la emisión de un certificado ante la Autoridad de Registro de la ACRN, presentando la información requerida (ver 3.1 - Registro Inicial).

La Autoridad de Registro de la ACRN debe validar la información presentada, y la generación de las claves debe satisfacer los requerimientos de seguridad y controles estipulados en la Declaración de Prácticas de Certificación de la ACRN.

4.2 - Procesamiento de Solicitud de Certificado

La ACRN deberá validar el CSR emitido por el PSCA. Para dicha verificación, la ACRN debe comprobar que:

a) la información contenida en el CSR es consistente con la información de acreditación ante la UCE;

b) el CSR se encuentra firmado con la clave privada correspondiente a la clave pública en él contenida;

c) existen pruebas fehacientes de que la clave privada con que se firmó el CSR está en exclusivo poder del PSCA, y que además ésta fue generada de acuerdo a los requerimientos estipulados en la sección 6.1.2 de la presente Política. Para este punto es suficiente una declaración de conformidad por parte del funcionario designado para presenciar la generación, o por los auditores designados para tal tarea;

d) el CSR contiene los campos requeridos por la presente Política de Certificación, de acuerdo a lo estipulado en el Punto 7 – Perfiles de Certificados y Listas de Certificados Revocados.

Si la verificación es satisfactoria, se da inicio a la Emisión de Certificado.

4.3 - Emisión de Certificado

La emisión del certificado se debe realizar en las instalaciones de la ACRN, y estará a cargo de personal técnico calificado y autorizado para tales efectos.

El período de validez del certificado emitido deberá ser el período comprendido entre la fecha de emisión y la fecha de expiración del certificado de la ACRN, excepto que sea revocado con anterioridad dicha fecha. Sin perjuicio de lo establecido, en caso que la evolución tecnológica pueda generar riesgo criptográfico, obsolescencia de sistemas o problemáticas afines, la UCE podrá determinar por vía regulatoria la obligatoriedad de efectuar las adecuaciones que entienda pertinentes.

4.4 - Aceptación del Certificado

El PSCA procede a la validación del mismo. Verifica que la información contenida en el certificado y la firma de la ACRN sean correctas.

En caso de que el PSCA acepte el certificado, deberá entregar a la ACRN el Acuerdo de Suscriptores firmado por su representante legal en un plazo no menor a veinticuatro horas (24) y proceder a la instalación del certificado en su ACPA en presencia del funcionario de la ACRN que lo entregó. En caso contrario se deberá proceder a la modificación del certificado, o a la revocación del mismo dependiendo de la magnitud de la discordancia.

La ACRN deberá publicar el certificado emitido, junto a la información de contacto del PSCA, en su repositorio público de información. A partir de dicha instancia se considera válida la operación de la ACPA.

Se publicará el certificado emitido, junto a la información de contacto del PSCA, en el repositorio público de información de la UCE, y se publicará al menos un (1) día en el Diario Oficial una referencia a dicha información.

4.5 - Uso del Certificado y del Par de Llaves

El PSCA debe utilizar la clave privada asociada al certificado emitido por la ACRN únicamente para firmar los certificados emitidos por su ACPA y la Lista de Revocación de Certificados bajo las Políticas de Certificación para las que fue acreditado por la UCE.

En ningún caso se encuentra autorizado el uso de la llave privada asociada al certificado para firmar otros documentos, cifrar información o realizar funciones de autenticación. La utilización de dicha llave para otro fin puede ser causal de revocación del certificado y/o suspensión de la acreditación del PSC.

El PSCA deberá mantener el certificado público emitido por la ACRN bajo la presente Política de Certificación en un repositorio público de información.

El PSCA deberá tomar las medidas de seguridad especificadas en la presente Política y en la Declaración de Prácticas de Certificación de la ACRN para la protección de la llave privada.

4.6 - Renovación del Certificado

La Renovación del Certificado es el proceso en el que la ACRN emite un nuevo certificado a la ACPA para que continúe sus operaciones una vez vencido el certificado anterior. No está permitido mantener el mismo par de llaves para diferentes certificados, por lo que el PSCA debe generar un par de llaves nuevo, con los requerimientos de seguridad definidos para la emisión de certificados (Ver 4.1).

Para la renovación del certificado, el PSCA debe presentar una constancia de acreditación emitida por la UCE con vigencia a la fecha en que se realice la solicitud. La solicitud debe ser presentada a la Autoridad de Registro de la ACRN, la cual deberá validarla en conformidad con lo establecido en el punto 3.1.

Un PSCA podrá solicitar la emisión de un nuevo certificado con una antelación máxima de un (1) año antes de que expire el que posee. Luego de la emisión del nuevo certificado y hasta la expiración del anterior, el PSCA podrá operar con los dos certificados. El certificado anterior podrá ser utilizado únicamente para firmar la Lista de Revocación de Certificados correspondiente y validar la cadena de confianza de PKI Uruguay. El nuevo certificado podrá ser utilizado para las operaciones de emisión de nuevos certificados y firma de la nueva Lista de Revocación de Certificados.

4.7 - Cambio de Clave del Certificado

El Cambio de Clave del certificado no es un procedimiento permitido. Debe en su lugar aplicarse los procedimientos de Revocación y Emisión de Certificado en el mencionado orden.

4.8 - Modificación del Certificado

La Modificación del Certificado es permitida únicamente en el caso en que la ACRN emitiera un certificado con información errónea o imprecisa debido a un error interno y no a la información provista por el PSCA, y debe ser solicitada por el PSCA previamente a la aceptación formal del certificado. En cualquier otro caso, deben aplicarse los procedimientos de Revocación y Emisión de Certificado en el mencionado orden.

4.9 - Suspensión y Revocación del Certificado

4.9.1 - Revocación del Certificado

La Revocación del Certificado es un procedimiento que anula definitivamente la validez de un certificado emitido por la ACRN, independientemente de su fecha de expiración. Para la Revocación, la ACRN agrega a su CRL el identificador del certificado revocado y la fecha de revocación.

En caso que el PSC pretenda continuar prestando servicios de certificación dentro de PKI Uruguay luego de la revocación, deberá acreditarse nuevamente ante la UCE.

Las causales para la revocación del certificado son las siguientes:

a) cuando existan evidencias de que la clave privada de la ACPA se encuentre comprometida, en un medio de almacenamiento comprometido o con riesgo cierto de estarlo;

b) si se constata un incumplimiento grave de las Políticas de Certificación para las cuales emite certificados y/o las Prácticas de Certificación por las cuales se debe regir;

c) si se constata que el PSCA está haciendo usos del certificado no permitidos por la presente Política de Certificación o las Políticas de Certificación según las cuales emite certificados;

d) si es revocada la acreditación del PSC por resolución de la UCE;

e) si el PSCA desea finalizar las operaciones de alguna de sus ACPA;

f) por resolución de una autoridad judicial competente;

g) otras causales especificadas en regulaciones emitidas por la UCE.

La UCE será quien disponga la revocación de un certificado, por resolución propia, a solicitud de un PSCA, a solicitud de la ACRN o a solicitud de una autoridad judicial competente.

En el caso de que el PSCA realice la solicitud de revocación, debe emitir una constancia escrita y aprobada por su representante legal para informar a la UCE. De ser aceptada y debidamente autenticada (ver 3.1.4), la UCE dispondrá la revocación. La UCE autoriza a la Autoridad de Registro de la ACRN para atender solicitudes de revocación de PSCA en escenarios de urgencia por motivos de seguridad, informando luego a la misma.

La ACRN tiene un período máximo de un (1) día a partir de la resolución de la UCE para revocar el certificado y publicar la CRL actualizada en el repositorio público de información.

El PSCA tiene un plazo máximo de un (1) día a partir de la revocación efectiva de su certificado para revocar todos los certificados emitidos con él y publicar una CRL o actualizar las bases de datos OCSP. Finalizado este procedimiento, el PSCA procederá a la destrucción de su clave privada mediante un mecanismo que impida su reconstrucción, para evitar compromisos futuros de esa clave. Este proceso deberá ser presenciado por un representante de la ACRN.

El PSCA, en caso de continuar sus operaciones, debe mantener publicada la CRL con todos los certificados revocados, y mantener disponible la base de datos OCSP si contara con una. Además deberá realizar nuevamente el proceso de acreditación ante la UCE.

4.9.2 - Suspensión del certificado

La suspensión de certificados emitidos por la ACRN no es un proceso permitido.

4.9.3 - Suspensión de PSCA o ACPA

La suspensión de un PSCA o de una ACPA es un proceso mediante el cual se prohíbe que ésta emita certificados electrónicos por el tiempo que dure la suspensión.

Una suspensión puede dar lugar a una revocación del certificado de la ACPA, si la UCE lo considera pertinente.

Las causales para la suspensión son las siguientes:

a) si se constata que la información contenida en el certificado es errónea o se encuentra desactualizada;

b) si se determina que existieron errores en los procedimientos operativos asociados a la emisión del certificado;

c) si se realizan cambios significativos en la presente Política de Certificación;

d) por resolución de una autoridad judicial competente;

e) otras causales especificadas en regulaciones emitidas por la UCE.

4.10 - Servicio de estado de los Certificados

La ACRN deberá publicar en su Repositorio de información los certificados emitidos, así como también la CRL correspondiente para su consulta online,

Ni la ACRN ni la UCE se responsabilizan por ningún tipo de incidente que derive de una falta de verificación de la CRL de la ACPA en el momento de validación de un certificado por parte de los Terceros aceptantes.

La ACRN deberá garantizar alta disponibilidad de la información, a excepción de los períodos planificados de mantenimiento.

La ACRN publicará esta información en www.agesic.gub.uy/acrn/acrn.html, y deberá especificar la URL concreta de publicación de estos servicios en su CPS.

4.11 - Finalización de la Suscripción

La finalización de la suscripción refiere a las situaciones en las que el certificado alcance su fecha de expiración, en que la ACRN finalice sus servicios o en que la ACPA finalice sus servicios.

En el caso de que el certificado alcance su fecha de expiración, ningún Tercero aceptante deberá confiar en él y la ACPA no deberá continuar utilizándolo para sus operaciones. Las operaciones realizadas con anterioridad a la fecha de expiración mantienen validez.

La ACRN deberá especificar en su Declaración de Prácticas de Certificación el procedimiento para el eventual cese de sus actividades.

En la eventualidad de que un PSCA finalice sus servicios o finalice los servicios de una de sus ACPA:

a) el PSCA deberá publicar la fecha de suspensión de las actividades de la ACPA con sesenta (60) días de antelación en su Sitio Oficial y una referencia a dicha información en el Diario Oficial durante un (1) día hábil;

b) el PSCA deberá notificar a los suscriptores de los certificados emitidos por la ACPA en un plazo menor a quince (15) días luego de anunciada su suspensión en su Sitio Oficial y en el Diario Oficial;

c) la UCE procederá a la suspensión de la ACPA del PSCA, inhabilitándola a emitir y/o renovar certificados;

d) luego de expirados todos los certificados de suscriptores de la ACPA, el PSCA deberá proceder a la destrucción de la clave privada de la ACPA mediante un mecanismo que impida su reconstrucción, según fue especificado en su Declaración de Prácticas de Certificación;

e) la UCE publicará en su Sitio Oficial, y una referencia en el Diario Oficial, el cese total de actividades de la ACPA del PSCA;

f) el certificado de la ACPA, el directorio de certificados emitidos por ella y la última lista de revocación emitida deberán ser transferidos a la UCE;

g) la UCE publicará en su Sitio Oficial, y una referencia en el Diario Oficial, el enlace al sitio donde se encuentra la lista de revocación y el certificado de la ACPA que finalizó sus operaciones.

Luego de la suspensión de la ACPA del PSCA (numeral c), esta no podrá emitir ningún certificado pero deberá continuar dando soporte a las operaciones de revocación y publicación según se establece en el punto 4.9.2. Los suscriptores podrán continuar utilizando certificados emitidos por esa ACPA hasta la fecha de expiración de los mismos o hasta que fueran revocados. El PSCA tiene la obligación de mantener los servicios de revocación de certificados, publicación de CRL y/o validación OCSP durante ese lapso. Una vez expirados o revocados todos los certificados, y luego de notificada la UCE, cesa automáticamente la responsabilidad del PSCA para esa ACPA.

En caso de que el PSCA no pueda mantener la actividad de la ACPA durante el período de suspensión, quedan a criterio de la UCE las acciones a tomar.

4.12 - Recuperación y Escrow de la Llave

Los PSCA, como Suscriptores de los certificados emitidos bajo la presente Política de Certificación, están autorizados a contratar servicios de *escrow* como respaldo para su clave privada. Los requerimientos para brindar servicios de escrowing de clave privada

se encuentran publicados en el documento “Requerimientos para depositarios de clave privada de ACPA mediante escrow”, publicado en www.uce.gub.uy/informacion-tecnica/prestadores.

Los PSCA se encuentran autorizados a almacenar copias de seguridad de su clave privada tomando las medidas de protección técnicas y físicas correspondientes (ver 6.2 – Protección de llave privada y controles de Módulos Criptográficos).

La recuperación de la clave privada, para continuar utilizando el mismo certificado, puede realizarse únicamente en los casos en los que la clave en posesión del PSCA haya sido destruida, por ejemplo por fallas de hardware. El PSCA deberá notificar a la UCE de la situación y la ACRN deberá comprobar fehacientemente que no es posible reconstruir la clave privada y que no hay riesgo de que la misma se encuentre comprometida. Debe encontrarse presente personal designado por la ACRN en el procedimiento de recuperación de la clave.

5 - Controles administrativos, operativos y físicos

El objetivo de los controles administrativos, operativos y físicos es implementar medidas de protección para la clave privada utilizada por la ACRN, la información de los PSCA y el ciclo de vida de los certificados emitidos por la ACRN y por las ACPA.

Los controles Administrativos, operativos y físicos deben estar documentados para su uso interno, y en la CPS de la Autoridad de Certificación (ACRN o ACPA) debe especificarse un resumen. La CPS estará sujeta a la aprobación de la UCE durante la acreditación inicial, mientras que la documentación interna estará sujeta a auditorías periódicas. Dichas medidas deben incluir, pero sin restringirse a:

a) Controles de seguridad física: La ACRN y las ACPA deberán implementar sólidas medidas de seguridad física para la protección de su equipamiento e instalaciones, tanto de accesos no autorizados como de siniestros como incendios e inundaciones.

b) Controles Procedimentales: Los procesos que permiten el funcionamiento de la ACRN y las ACPA deberán estar documentados y deberán basarse en la contraposición de intereses para sus operaciones más críticas, interviniendo varias personas durante la solicitud, aprobación, ejecución y control de las tareas desarrolladas. Para aquellas tareas críticas como la gestión de la clave privada de la autoridad certificante, deben implementarse medidas de división del conocimiento y contraposición de intereses.

c) Seguridad ligada al Personal: Los requerimientos de seguridad ligada al personal que empleen tanto la ACRN como las ACPA, deberán estar documentados, y además deberán estar especificados en sus respectivas Declaraciones de Prácticas de Certificación.

d) Registros de Auditoría: Tanto la ACRN como las ACPA deben tener definida una política de registros de auditoría (*logs*) que defina qué o*peraciones* se registran y c*ómo se* garantiza la integridad de esos registros. Mínimamente se deben registrar todas las actividades relativas a la gestión de claves (generación, destrucción, activación, desactivación, etc.), a la gestión de certificados (emisión, revocación, renovación, etc.) y a la emisión de CRLs y/o respuestas a consultas OCSP.

e) Retención de Registros e Información: Para cada tipo de registro se debe especificar además qué política de retención se va a aplicar. Los registros

relativos a la generación de claves y emisión/renovación de certificados deben mantenerse mínimamente hasta que el certificado expira o es revocado. Los registros relativos a las demás operativas deben mantenerse por al menos un (1) año. Los certificados emitidos por una autoridad certificadora deben ser mantenidos en su directorio público por tiempo indefinido, incluso luego de su expiración y/o revocación

f) Cambio de Claves: El cambio de claves no está permitido para la ACRN ni para las ACPA.

g) Continuidad de Operaciones: Tanto la ACRN como las ACPA deberán tener definidos planes de continuidad del negocio y recuperación ante desastres, que le permitan continuar con su operativa en la eventualidad de fallas de equipamiento y/o siniestros. El nivel mínimo de funcionamiento exigido para una autoridad certificadora en la PKI Uruguay es el de la atención de pedidos de revocación de certificados y provisión de los servicios de consulta de validez de los mismos.

h) Terminación de las Operaciones.

6 – Controles de Seguridad Técnica

Los controles técnicos descriptos en esta sección tienen el objetivo de proteger el par de llaves de la ACRN y de las ACPA durante su ciclo de vida. Se especifican además medidas generales para la protección de los sistemas de información que dan soporte a las actividades de la ACRN y las ACPA.

6.1 – Instalación de equipamiento de la CA

6.1.1 – Autoridad Certificadora Raíz Nacional

La instalación de los sistemas de CA de la ACRN se debe realizar durante la Ceremonia de Generación de Llaves de la ACRN. Durante dicho evento se instalan completamente los sistemas sobre el hardware de producción, y los requerimientos de atestiguamiento se detallan en el punto 6.2.1.

6.1.2 – Autoridad Certificadora del Prestador Acreditado

El equipamiento dedicado a la gestión de certificados del Prestador Acreditado (la CA misma) debe ser instalado en presencia de auditores autorizados, de forma de certificar su correcta instalación. Los PSCA podrán instalar su equipamiento en una fecha dada en presencia de auditores autorizados, y extraer del equipamiento una imagen de la instalación, la cual deberá ser enviada a la UCE y permanecer en poder de la misma hasta el momento de su ceremonia de generación de llaves. La misma también deberá ser auditada, y comprenderá el proceso de instalación de la imagen en los sistemas además de la posterior generación de los pares de llaves, tal como se expresa en el punto 6.2.2.

6.2 – Generación e Instalación de pares de llaves

6.2.1 – Autoridad Certificadora Raíz Nacional

El par de llaves de la ACRN deberá ser generado durante la Ceremonia de Generación de Llaves. Dicha ceremonia se realiza en las instalaciones designadas por la AGESIC para la operación de la ACRN, bajo aprobación explícita de la UCE, respetando los

requerimientos de la CPS de la ACRN y de acuerdo a lo estipulado en el Guión de la Ceremonia de Claves.

6.2.2 – Autoridad Certificadora del Prestador Acreditado

El acto de generación del par de llaves para la ACPA se debe realizar en las instalaciones del PSCA, en presencia de un funcionario designado por la ACRN y de acuerdo a los requerimientos estipulados por la presente Política de Certificación (ver 4.1 - Solicitud de Certificado).

El PSCA debe contar con la infraestructura donde serán generadas las llaves previamente configurada y las medidas de protección requeridas por la presente Política ya implementadas.

La generación del par de llaves debe realizarse en un módulo criptográfico seguro.

La llave generada deberá ser RSA de 4096 bits.

El PSCA debe elaborar previamente una guía donde se describa el procedimiento de generación de llaves y exportación del CSR. Deben especificarse en dicha guía las responsabilidades, pasos a seguir y registros formales de su ejecución.

Al finalizar el procedimiento, el funcionario designado por la ACRN debe retirar de las instalaciones del PSCA el CSR para ser posteriormente utilizado en la emisión del certificado.

6.3 – Protección de llave privada y controles de Módulos Criptográficos

La ACRN debe publicar su clave pública en su repositorio de información. Se deben tomar medidas de protección adecuadas a nivel de sistemas para asegurar su integridad. La protección de la llave privada de la ACRN y de las ACPA debe realizarse con módulos criptográficos (HSM) que cumplan con la normativa FIPS 140-2 nivel 3.

Las llaves privadas de la ACRN y de la ACPA pueden encontrarse únicamente cifradas bajo claves generadas y residentes en los módulos criptográficos (llaves maestras). El equipamiento de producción y el de contingencia (que es recomendable tener) deben contar con los controles de seguridad físicos y lógicos requeridos por esta Política de Certificación.

La llave maestra de la ACRN y de las ACPA no puede ser retirada de los módulos criptográficos en claro (sin cifrado). El cifrado a utilizar debe ser AES 256 o 3DES con clave de largo triple. El retiro de la llave maestra de los módulos de criptografía puede realizarse únicamente para procedimientos de respaldo de la llave, procedimientos de *escrow* (para el caso de las ACPA) y para el cambio de módulo criptográfico. Estos procedimientos deben ser aprobados y controlados según sea requerido en cada caso, por la UCE para el caso de la ACRN, y por la ACRN para el caso de las ACPA.

Las llaves maestras de un módulo criptográfico HSM que sean retiradas deben cifrarse con criptografía sólida, especificada en la CPS de la ACRN o de la ACPA según corresponda. La clave utilizada para la protección de la llave maestra retirada debe encontrarse dividida entre al menos 3 custodios, siendo cada custodio designado por la ACRN o la ACPA –según corresponda– y considerando la contraposición de intereses.

El *escrow* de la llave maestra de las ACPA debe realizarse mediante un medio impreso con la llave codificada en base64. Ninguna persona ajena a la entidad que realiza el *escrow* puede tener acceso completo a ver o retener la clave maestra. Los procedimientos para *escrow* de llaves privadas son los detallados en la presente política (ver 4.12 - Recuperación y Escrow de la Llave).

Para que el respaldo o *escrow* de una clave privada sea efectivo, debe respaldarse la llave maestra del módulo criptográfico y la clave privada cifrada por dicha llave, o solo la llave privada en forma cifrada si el modelo particular de HSM no maneja llaves maestras.

Una vez que el certificado de la ACRN o de la ACPA haya expirado, debe procederse a la destrucción de la clave privada y de la clave maestra del módulo criptográfico. La destrucción debe realizarse con un mecanismo que impida su recuperación. En caso de que se haya realizado *escrow* en un medio impreso, el método de destrucción es su incineración. En caso de una *smart-card*, debe destruirse físicamente de forma que no pueda ser reconstruida. El módulo de criptografía utilizado debe proveer funciones para la eliminación segura de la llave maestra.

La destrucción de la clave privada de la ACRN debe realizarse según los procedimientos estipulados en su CPS.

La destrucción de la clave privada de la ACPA es responsabilidad del PSCA acreditado. El PSCA debe contar con procedimientos para tales fines especificados en su Declaración de Prácticas de Certificación y, por lo tanto, aprobados por la UCE en el proceso de acreditación.

6.4 – Otros aspectos de gestión de llaves

La ACRN y los PSCA deberán mantener un archivo de todos los certificados que contengan claves públicas utilizadas para la emisión de certificados, es decir, todos los certificados alguna vez utilizados por sus Autoridades de Certificación. De esta forma, es posible validar las cadenas de confianza en las que participan la ACRN o las ACPA para cualquier instante de tiempo.

El período de validez máximo del certificado de la ACRN es de veinte (20) años.

El período de validez máximo de los certificados emitidos por la ACRN bajo la presente Política de Certificación (certificados de las ACPA) es el máximo posible al momento de la emisión, según la fecha de expiración del certificado de la ACRN (ver 4.3 - Emisión de Certificado).

El período de validez máximo del par de llaves de la ACRN o de la ACPA es el de su certificado. Transcurrido dicho período o en caso de revocación del certificado, la llave privada correspondiente a la llave pública contenida en el certificado debe ser eliminada (ver 6.2 – Protección de la llave privada y controles de Módulos Criptográficos).

6.5 – Datos de activación

Para la activación de las llaves privadas de la ACRN y de la ACPA se requiere la participación de varios individuos (custodios) en un esquema “N de M”. Esta división del conocimiento impide que un individuo por sí solo tenga el conocimiento suficiente para activar la llave privada. Para la ACRN N no deberá ser menor a tres, mientras que para las ACPA no deberá ser menor a dos.

Se entiende por “activación” al proceso previo a la utilización de la llave privada que permite, mediante un mecanismo de autenticación, hacerla disponible para ser usada. Esto implica que la llave privada sea usada múltiples veces tras un único proceso de autenticación. La activación puede realizarse por ejemplo al iniciar el sistema. En el caso de las ACPA, se activa la llave privada al comenzar las actividades de emisión de certificados o CRLs firmadas.

Cuando la llave privada no sea utilizada o se cumpla alguna de las condiciones establecidas, debe ser desactivada. Se entiende por “desactivación” cualquier proceso que haga *imprescindible* volver a activar la clave privada para utilizarla. Por ejemplo, puede definirse que tras determinado período de inactividad del sistema o al apagarlo, se desactive la llave privada. En el caso de las ACPA, esto puede darse en el reinicio del sistema de emisión de certificados o en la suspensión del servicio por operaciones de mantenimiento. Los PSCA deben definir las condiciones para la desactivación de la

llave privada en su Declaración de Prácticas de Certificación. Estas condiciones deben ser lo más restrictivas posibles de forma tal de evitar que la llave privada se encuentre activada mientras no esté siendo utilizada.

En la ACRN la llave privada debe activarse al iniciar el sistema para emitir una CRL o un certificado. La desactivación debe realizarse tras la emisión de la CRL o del certificado.

Los datos para la activación de una clave privada pueden ser un PIN, *token* o *passphrase*.

6.6 – Seguridad computacional

La ACRN y la ACPA deben implementar políticas, estándares y procedimientos que permitan una operación segura.

Se deben instrumentar como mínimo los siguientes aspectos:

a) Definición de roles y responsabilidades;

b) Clasificación de la información;

c) Seguridad vinculada a los recursos humanos;

d) Seguridad lógica de los sistemas y redes;

e) Control del acceso lógico;

f) Seguridad física del ambiente y de los sistemas;

g) Gestión de respaldos;

h) Continuidad de la operativa y disponibilidad;

i) Registros de auditoría;

j) Respuesta a incidentes.

Estos controles serán objeto de regulación por parte de la UCE para la obtención y mantenimiento de la acreditación como PSCA.

6.7 – Controles de seguridad sobre el ciclo de vida de los sistemas

Debe existir un inventario actualizado con los sistemas de información y medios de almacenamiento asociados a la operativa de la ACRN y de las ACPA. Todos los medios a ser incorporados, retirados o trasladados fuera de las fronteras de la organización deben estar sujetos a previa autorización de la gerencia, en procedimientos definidos para ello. Dicho inventario debe ser mantenido por la ACRN y la ACPA en forma privada, y revelado sólo a los encargados de la auditoría, es decir, no forma parte de la información a publicar.

Estos controles serán objeto de regulación por parte de la UCE para la obtención y mantenimiento de la acreditación como PSCA.

6.8 – Seguridad de la red

Deben implementarse medidas adecuadas de protección para la operación de la ACRN y las ACPA si se encuentran conectadas en red. Por ejemplo, división de la red de la organización en capas, ubicando la ACPA en un segmento crítico al que no sea posible el acceso desde Internet. Si la Autoridad de Registro de la ACPA cuenta con un portal *online* y además está conectada a la ACPA para la emisión de certificados *online*, esta conexión debe estar sujeta a estrictos controles de seguridad a nivel de red, como por ejemplo mediante firewalls, controles de acceso y auditoría (logs).

Estos controles serán objeto de regulación por parte de la UCE para la obtención y mantenimiento de la acreditación como PSCA.

6.9 – Sincronización Horaria

La ACRN y las ACPA deben utilizar la fecha y hora de la República Oriental del Uruguay al firmar los certificados que emiten, con un margen de error máximo del orden del minuto.

7 – Perfil de certificados y de Listas de certificados revocados

El formato del certificado cumple con lo especificado en el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), mientras que la lista de revocación de certificados cumple con el mismo estándar, pero en su versión 2. Ambos están definidos en su versión más reciente en el RFC 5280.

7.1 – Perfil del Certificado de la ACRN

Se utilizarán los siguientes campos del formato X.509 versión 3:

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACRN
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Validez (Valid From / Valid To)	20 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 4096 bits
Extensiones	
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Uso de Claves (Key Usage)	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1

	CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.0 URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf OID: 2.16.858.10000157.66565.1 URI: www.agesic.gub.uy/acrn/cps_acrn.pdf
Restricciones Básicas (Basic Constraints)	CA = TRUE Largo indefinido
Puntos de distribución de las CRL (CRL Distribution Points)	URI = www.agesic.gub.uy/acrn/acrn.crl URI = www.uce.gub.uy/acrn/acrn.crl

7.2 – Perfil del Certificado de las ACPA

Se utilizarán los siguientes campos del formato X.509 versión 3:

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACRN
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Validez (Valid From / Valid To)	Período de validez asignado al momento de la emisión (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	Nombre Distinguido de la ACPA según lo establecido en el punto 3.1.1
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 4096 bits

Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Identificador de la clave pública de la ACRN
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Uso de Claves (Key Usage)	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.0 URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf OID: 2.16.858.10000157.66565.1 URI: www.agesic.gub.uy/acrn/cps_acrn.pdf
Restricciones Básicas (Basic Constraints)	CA = TRUE Largo 0
Puntos de distribución de las CRL (CRL Distribution Points)	URI = www.agesic.gub.uy/acrn/acrn.crl URI = www.uce.gub.uy/acrn/acrn.crl
Información de Acceso de la Autoridad Certificadora (Authority Information Access)	URI = www.agesic.gub.uy/acrn/acrn.cer

7.3 – Perfil de la CRL de la ACRN

Se utilizarán los siguientes campos del formato X.509 versión 2:

Atributos	Contenido
Versión (Version)	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA

Nombre Distintivo del Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Día y Hora de Emisión (Efective Date)	Día y hora de la emisión de esta CRL
Próxima Actualización (Next Update)	Día y hora de la próxima actualización planificada de la CRL (3 meses)
Certificados Revocados (Revoked Certificates)	Lista de los certificados revocados. Incluye número de serie (Serial Number) y fecha de revocación (Revocation Date).
Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Identificador de la clave pública de la ACRN
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

8 – Administración Documental

8.1 – Procedimiento para cambio de especificaciones

La UCE cuenta con procedimientos internos para la administración de los cambios sobre la presente Política de Certificación.

8.2 – Procedimientos de Publicación y Notificación

La UCE publicará en su sitio web las modificaciones aprobadas a la presente Política de Certificación, indicando en cada caso las secciones y/o textos reemplazados junto con la publicación de la nueva versión. Además, publicará un vínculo a los mismos en el Diario Oficial durante un (1) día hábil.

Lo anteriormente estipulado también aplica al Acuerdo con Suscriptores de Certificados. Los PSCA serán notificados directamente ante cualquier cambio en estos términos o en la presente Política de Certificación.