Declaración de Prácticas de Certificación de la Autoridad Certificadora Raíz Nacional

Autoridad Certificadora Raíz Nacional

AGESIC

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 presente Declaración de Prácticas de Certificación contiene las prácticas empleadas por la AGESIC en la ACRN para la gestión de certificados y CRL.

1.2 - Identificación de la Declaración de Prácticas de Certificación

Nombre: Declaración de Prácticas de Certificación de la ACRN

Versión: 1.0

Fecha de elaboración: 25/10/2011

Fecha de última actualización: 25/10/2011

OID: 2.16.858.10000157.66565.1

Sitio web de publicación: www.agesic.gub.uy/acrn/cps_acrn.pdf

1.3 - Participantes de la PKI Uruguay

1.3.1 – Unidad Reguladora

El rol de Unidad Reguladora en PKI Uruguay es desempeñado por la UCE, y sus funciones están estipuladas en la Política de Certificación de la ACRN.

1.3.2 - Autoridad de certificación

El rol de Autoridad de Certificación Raíz Nacional (ACRN) es desempeñado por la AGESIC, y sus funciones están estipuladas en la Política de Certificación de la ACRN.

1.3.3 - Autoridad de Registro

El rol de Autoridad de Registro para la ACRN es desempeñado por la AGESIC, y sus funciones están estipuladas en la Política de Certificación de la ACRN.

1.3.4 - Suscriptores

Los suscriptores de los certificados emitidos por la ACRN son los PSCA, y sus funciones se encuentran detalladas en la Política de Certificación de la ACRN.

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 Política de Certificación de la ACRN y según la presente Declaración de Prácticas de Certificación. 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 Política de Certificación de la ACRN y de acuerdo a la presente Declaración de Prácticas 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 Política de Certificación de la ACRN).

1.5 - Administración de la Declaración de Prácticas

La Administración de la presente Declaración de Prácticas de Certificación es responsabilidad de la AGESIC.

Por consulta o sugerencias, la AGESIC designa al siguiente contacto:

Nombre: AGESIC

Dirección de correo: acrn@agesic.gub.uy

Teléfono: (+598) 2901 2929

1.5.1 - Procedimiento de aprobación

El sistema documental y de organización de la ACRN garantiza, a través de la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de esta Declaración de Prácticas de Certificación y de las especificaciones de servicios que están relacionados. Se prevé, de esta forma, el procedimiento de modificación de especificaciones del servicio y el procedimiento de publicación de especificaciones del servicio. Las modificaciones finales de la Declaración de Prácticas de Certificación son aprobadas por la AGESIC una vez haya

sido comprobado el cumplimiento de los requerimientos establecidos en las diferentes secciones de la presente Declaración de Prácticas de Certificación.

1.6 - Definiciones y abreviaturas

Unidad de Certificación Electrónica (UCE): órgano desconcentrado de AGESIC, creado por el artículo 12 de la Lay 18.600 de Documento Electrónico y Firma Electrónica. Sus cometidos detallados pueden consultarse en la referida Ley, o en la Política de Certificación de la ACRN.

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 en el que solicita y provee información a la ACRN para la emisión de un certificado firmado por ella.

PKCS#10: Estándar para criptografía de clave pública que describe el formato de los mensajes con los que se solicita la emisión de un certificado. Contiene generalmente la identidad y clave pública del solicitante.

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

Estipulado en la Política de Certificación de la ACRN.

2.2. - Responsabilidades

Estipulado en la Política de Certificación de la ACRN

2.3. - Interpretación y aplicación de las normas

Estipulado en la Política de Certificación de la ACRN.

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

2.4.1. - Publicación de información del certificador

La ACRN dispone del siguiente sitio web como repositorio público de información:

- www.agesic.gub.uy/acrn/acrn.html

Este servicio de publicación de información del certificador está disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la AGESIC, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

La información mínima que la UCE y la ACRN publican en los sitios webs está estipulada en la sección 2.1.6 de la Política de Certificación de la ACRN, e incluye lo siguiente:

- Las listas de certificados revocados y otras informaciones sobre el estado de revocación de los certificados;

- La Política de Certificación y, cuando sea conveniente, las políticas específicas de la ACRN;
- Los perfiles de los certificados y de las listas de revocación de los certificados;
- La Declaración de Prácticas de Certificación; y,
- Los instrumentos jurídicos vinculados con los Prestadores de Servicios de Certificación Acreditados y de los Terceros aceptantes.

2.4.2. - Frecuencia de publicación

La AGESIC cumple con las frecuencias estipuladas en la Política de Certificación de la ACRN.

2.4.3. - Controles de acceso a la información

La ACRN brinda acceso irrestricto a toda la información contenida en el repositorio público (ver 2.1.6 de la Política de Certificación de la ACRN), 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 ACRN están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la AGESIC, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

2.5. - Auditorías

La AGESIC cumple con lo estipulado en la Política de Certificación de la ACRN.

2.6. - Confidencialidad

A los efectos de la determinación del carácter de confidencial de la información recibida por la ACRN se estará a los recaudos previstos de acuerdo con lo establecido en la Ley Nº 18.381, del 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 ACRN:

a) Los datos de contacto de los PSCA;

b) Los certificados electrónicos emitidos para sus ACPA.

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 se publica por la ACRN a través de su CRL, disponible en el sitio www.agesic.gub.uy/acrn/arcn.crl. Las razones que dan lugar a una revocación se consideran públicas, y se incluyen en el repositorio público de la UCE (www.uce.gub.uy/informacion-tecnica/prestadores).

La información sobre el estado de suspensión de un PSCA es competencia de la UCE, y su tratamiento se estipula en la Política de Certificación de la ACRN.

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 ACRN divulgue información.

2.7. - Derechos de Propiedad Intelectual

La AGESIC mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la presente documentación y aplicaciones pertenecientes a ella. Ninguna parte de este documento se puede reproducir o distribuir sin que la previa notificación de derechos de propiedad intelectual aparezca en forma precisa, completa y sin modificaciones, atribuyendo su autoría a la AGESIC.

3 - Identificación y Autenticación

3.1 – Registro Inicial

En el contexto de la presente Declaración de Prácticas, la Identificación y Autenticación comprende el proceso que va desde que el PSCA, acreditado ante la UCE, se presenta en la ACRN para solicitar su certificado, y el punto en el que la Autoridad de Registro de la ACRN valida su identidad y habilita la emisión de su certificado.

El PSCA podrá solicitar la emisión de los certificados ante la Autoridad de Registro de la ACRN. Dichos certificados son emitidos bajo la Política de Certificación de la ACRN y de acuerdo a la presente Declaración de Prácticas 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 de acuerdo a la presente Declaración de Prácticas 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

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 utiliza el campo “Subject” del certificado emitido por la ACRN (ver 7.2 de la Política de Certificación de la ACRN). El formato para indicar el nombre de la ACPA es X.500 (Distinguished Name).

El formato se aplica de acuerdo a lo estipulado en la sección 3.1.1 de la Política de Certificación de la ACRN.

3.1.2 - Validación Inicial de Identidad

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

3.1.2.1 - Acreditación

a) Tal como se estipula en la Política de Certificación de la ACRN, previo al proceso de registro, el PSC debe acreditarse ante la UCE para poder operar en el contexto de PKI Uruguay.

a) 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 vigente ante la UCE, deberá demostrar ante la Autoridad de Registro de la ACRN su identidad, de la siguiente forma:

a) nombres y apellidos,

b) documento de identidad.

La ACRN verifica que dichos datos además coincidan con los establecidos en la resolución de acreditación.

3.1.2.3 - Clave privada

Se cumple con lo estipulado en la Política de Certificación de la ACRN para este punto, designándose un funcionario de la ACRN para presenciar el acto de generación de llaves de ACPA.

3.1.3 - Identificación y Autenticación para Solicitudes de Cambio de Clave

No se realiza cambio de claves de las ACPA ni de la ACRN como proceso independiente. En caso de requerirse, se realiza 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 valida la identidad del solicitante previo a la solicitud de revocación del certificado emitido a una ACPA del PSCA.

Se verifica que el solicitante esté habilitado por la UCE para solicitar la revocación y se lo identifica oportunamente al igual que en el punto 3.1.2.2.

4 - Requerimientos Operativos del Ciclo de Vida de los Certificados

En esta sección se declaran los controles que realiza la ACRN para asegurar una gestión segura del Ciclo de Vida de los Certificados emitidos por ella, y también se especifican controles que los PSCA, como suscriptores de esos certificados, deben considerar.

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 valida la información presentada y verifica que la generación de las claves satisfaga los requerimientos de seguridad y controles estipulados en la presente Declaración de Prácticas de Certificación.

Para solicitar el certificado, el PSCA genera las claves de su ACPA en presencia de los funcionarios de la ACRN y de la UCE, y genera una solicitud en formato PKCS#10 (CSR). Dicha solicitud debe contener únicamente la clave pública generada y los datos del Distinguished Name de la ACPA, de acuerdo a lo estipulado en la sección 3.1.1 de la Política de Certificación de la ACRN, y en conformidad con los datos provistos a la UCE durante el proceso de acreditación. Además, debe estar firmada con la clave privada de la ACPA.

El CSR es entregado al funcionario de la ACRN en un medio removible autorizado y por él provisto, de forma de continuar con el proceso de emisión.

4.2 - Procesamiento de Solicitud de Certificado

La ACRN valida el CSR emitido por el PSCA en conformidad con lo estipulado en la Política de Certificación de la ACRN. Para dicha verificación, el operador de la ACRN a cargo de la emisión comprueba que:

a) la información de identificación de la ACPA 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) el funcionario que fue designado para presenciar el proceso de generación del par de llaves de ACPA expresó su conformidad con el mismo;

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

Si la verificación es satisfactoria, se da inicio a la Emisión de Certificado. En caso contrario, la emisión no tiene lugar y se notifica al PSCA y a la UCE los motivos.

4.3 - Emisión de Certificado

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

El período de validez del certificado emitido debe ser de diez (10) años, excepto que sea revocado con anterioridad a la fecha de expiración. Sin perjuicio de lo señalado, la evolución tecnológica puede determinar una regulación específica de la UCE, por lo que esta emisión no implica la constitución de derechos adquiridos por todo el período.

El certificado emitido es retirado del sistema donde fue generado en un dispositivo removible provisto por la ACRN. Este dispositivo es entregado al representante del PSCA, dejando una constancia formal del acto mediante la firma del Acuerdo para Suscriptores. Una copia del certificado es almacenada en el directorio de certificados de la ACRN. Esta copia no es publicada en el repositorio de información durante esta instancia.

4.4 - Aceptación del Certificado

El funcionario a cargo de la emisión del certificado se dirige a las instalaciones del PSCA y entrega personalmente el medio removible que contiene el certificado.

Al momento de entrega 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 dos horas y proceder a la instalación del certificado en su ACPA en presencia del funcionario de la ACRN que lo entregó. En caso contrario, se procede a la modificación del certificado, o a la revocación del mismo dependiendo de la magnitud de la discordancia.

La ACRN publica el certificado emitido, junto a la información de contacto del PSCA, en su repositorio público de información, y envía el certificado a la UCE para su publicación. A partir de dicha instancia se considera válida la operación de la ACPA.

4.5 - Uso del Certificado y del Par de Llaves

Estipulado en la Política de Certificación de la ACRN.

4.6 - Renovación del Certificado

Para la renovación del certificado, el PSCA debe presentar una constancia de acreditación vigente emitida por la UCE a la fecha en que se realice la solicitud. La solicitud debe ser presentada a la Autoridad de Registro de la ACRN, que la validará en conformidad con lo establecido en el punto 3.1. Para la renovación del certificado se deberá generar un nuevo par de llaves en todos los casos.

Otros requisitos para la renovación están estipulados en la Política de Certificación de la ACRN.

4.7 - Cambio de Clave del Certificado

No se realizan cambios de clave de Certificados. En caso de ser necesario, se aplican los procedimientos de Revocación y Emisión de Certificado en el orden mencionado, o de Renovación.

4.8 - Modificación del Certificado

Se cumple con lo estipulado en la Política de Certificación de la ACRN. Únicamente se atienden solicitudes de modificación cuando estas se realizan previo a la aceptación formal del certificado.

4.9 - Suspensión y Revocación del Certificado

4.9.1 - Revocación del Certificado

Para la Revocación, se agrega a la CRL el identificador del certificado revocado y la fecha de revocación.

Las causales para la revocación del certificado están estipuladas en la Política de Certificación de la ACRN.

La ACRN atiende pedidos de revocación directamente de la UCE.

Adicionalmente, la ACRN pedirá la revocación de un certificado de ACPA ante la UCE cuando constate que la misma ha incurrido en alguna de las causales de revocación.

La ACRN atiende pedidos de revocación de suscriptores en nombre de la UCE en escenarios de urgencia por motivos de seguridad, informando luego a la misma.

El proceso de revocación del certificado y publicación de la nueva CRL se realiza en un plazo no mayor a un (1) día a partir de la autenticación y aprobación de la solicitud de revocación del PSCA, sea esta emitida por la UCE o solicitada por el PSCA mismo.

Se dispondrá de un funcionario de la ACRN para presenciar el proceso de revocación efectiva de todos los certificados emitidos por una ACPA revocada, y también del proceso de destrucción efectiva de la calve privada asociada a la misma.

4.9.2 - Suspensión del certificado

No se realiza suspensión de certificados emitidos por la ACRN.

La Suspensión administrativa del PSCA es un proceso llevado a cabo por la UCE.

4.10 - Servicio de Estado de los Certificados

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

La ACRN no se responsabiliza 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.

Este servicio de publicación de información del certificador está disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la AGESIC, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

El Repositorio se encuentra en www.agesic.gub.uy/acrn/acrn.html.

La CRL se encuentra en www.agesic.gub.uy/acrn/acrn.crl y en www.uce.gub.uy/acrn/acrn.crl.

4.11 - Finalización de la Suscripción

En la eventualidad de que la ACRN finalice sus servicios:

a) se publicará la fecha de finalización con sesenta (60) días de antelación en el Sitio Oficial de la ACRN y un vínculo a dicha información en el Diario Oficial durante un (1) día hábil;

b) se notificará a los PSCA con al menos sesenta (60) días de antelación;

c) se procederá a la revocación de todos los certificados emitidos que se encuentren vigentes a la fecha de terminación;

d) se procederá a la destrucción de la clave privada de la ACRN mediante un mecanismo que impida su reconstrucción.

Los PSCA, como Suscriptores, no podrán continuar utilizando certificados emitidos por la ACRN y los Terceros aceptantes no deberán confiar en ellos.

El procedimiento para el cese de actividades de un PSCA está estipulado en la Política de Certificación de la ACRN.

4.12 - Recuperación y Escrow de la Llave

Estipulado en la Política de Certificación de la ACRN.

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.

Para esto, la ACRN cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI), con Políticas y Procedimientos para garantizar la seguridad en sus operaciones. Dicho SGSI está alineado con los requerimientos de WebTrust for Certification Authorities y con el código de buenas prácticas ISO 27002, y está enfocado a proteger el material criptográfico involucrado en el ciclo de vida de los certificados de la ACRN y de los PSCA.

5.1 - Controles de seguridad física

La ACRN implementa las siguientes medidas de seguridad para la protección física de las instalaciones donde se encuentran los sistemas informáticos asociados al ciclo de vida de los certificados emitidos:

a) delimitación de las áreas seguras e inseguras en las instalaciones donde se procesan o almacenan claves criptográficas y certificados;

b) medidas para impedir el acceso no autorizado a las instalaciones a través de puertas, ventanas y muros;

c) medidas de control de acceso físico que permiten identificar y autorizar a los individuos que ingresan y egresan de la organización (lectores biométricos, tarjetas de aproximación, guardias de seguridad);

d) medidas restrictivas para el acceso a las áreas seguras dentro de la organización (ingreso del mínimo personal requerido);

e) medidas de detección del acceso en áreas vacantes (sensores de movimientos, alarmas, cámaras de video);

f) medidas para el control de la temperatura del equipamiento en funcionamiento;

g) medidas de protección contra incendios (detectores de humo, extintores de polvo);

h) medidas de protección contra inundaciones (de acuerdo a la evaluación de riesgos de inundación);

i) utilización de cerraduras y *racks* cerrados para la protección de sistemas e información crítica.

Para la protección del equipamiento de las áreas de trabajo, se implementan las siguientes medidas:

a) Inventario actualizado de los sistemas y medios de almacenamiento de la organización;

b) procedimientos para el ingreso y egreso de sistemas y medios a la organización, que requieren la aprobación explícita de los niveles gerenciales;

c) procedimientos para la destrucción física de medios de almacenamiento;

d) política de escritorios limpios, retirando de las áreas de trabajo aquella información que no esté siendo utilizada;

e) separación entre los ambientes de producción, *backup* y *test*;

f) copias de seguridad periódicas almacenadas en instalaciones geográficamente distantes y bajo las mismas medidas de protección.

5.2 - Controles Procedimentales

Los procesos que permiten el funcionamiento de la ACRN se basan en la contraposición de intereses para sus operaciones más críticas, interviniendo varias personas durante la solicitud, aprobación, ejecución y control de las tareas desarrolladas. Se pueden identificar los siguientes roles en la operativa de la ACRN:

Gerente de Sistemas – Es el responsable de las decisiones de diseño y planificación de la infraestructura tecnológica para el soporte de las actividades de la autoridad certificadora. Se encarga de aprobar la incorporación de equipamiento, dispositivos de red y medios de almacenamiento, así como de software a ser utilizado durante el ciclo de vida de los certificados. El Gerente de Sistemas tiene también la responsabilidad de aprobar los procedimientos administrativos y técnicos destinados a mitigar los riesgos de seguridad asociados a la operativa. Además, define y aprueba el control de acceso lógico a los sistemas de información.

Administrador de Sistemas y Redes – Es el encargado de administrar los sistemas y dispositivos de comunicación. Ejecuta los procedimientos de instalación de software, instalación de dispositivos, configuración de sistemas.

Oficial de seguridad – Se encarga de dar soporte a la aplicación de los procedimientos administrativos definidos y asegurar su cumplimiento. Brinda apoyo a las decisiones gerenciales que impliquen cambios en el control del acceso, incorporación de equipamiento o cambios en el software. Realiza un seguimiento y participa durante el desarrollo de los planes de capacitación sobre seguridad de la información al personal de la organización.

Auditor – Tiene la función de controlar a través de registros de auditoría el cumplimiento con los procedimientos desarrollados. El rol de auditor está asignado a un individuo neutral e independiente de la organización.

Operador - Se encarga de la operación de los sistemas, ejecutando los procedimientos de emisión y revocación de certificados, emisión de CRL, etc.

Para aquellas tareas críticas como la gestión de la clave privada de la autoridad certificadora, se implementan medidas de división del conocimiento y contraposición de intereses.

5.3 - Seguridad asociada al Personal

La ACRN cumple con los siguientes requerimientos de seguridad asociados al Personal:

a) procedimientos para la incorporación de personal que permiten comprobar sus credenciales, referencias, antecedentes laborales y antecedentes judiciales (exclusivamente mediante el certificado de antecedentes judiciales que expide el Ministerio del Interior);

b) comunicación al individuo contratado o reasignado a otra área su rol y responsabilidades dentro de la organización;

c) exigencia al individuo contratado o reasignado a otra área la aceptación de las políticas de seguridad y de los acuerdos de confidencialidad;

d) planes de capacitación periódicos en seguridad de la información (específicos para cada rol) para todo el personal de la organización;

e) procedimientos para el retiro de personal de la organización.

5.4 – Registros de Auditoría

La ACRN tiene definida una política de registros de auditoría (*logs*) que define qué operaciones se registran y cómo se garantiza la integridad de esos registros.

Se registran 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.

Todos los registros se almacenan con la fecha en que fueron generados, la operación realizada, los objetos afectados, el resultado de dicha operación y la identificación del/los autores.

Los registros se almacenan de tal forma que se asegura su disponibilidad e integridad, impidiendo la modificación indebida, eliminación y su lectura.

5.5 – Retención de Registros e Información

Cada tipo de registro tiene definido el tiempo de retención. Los registros relativos a la generación de claves y emisión/renovación de certificados se almacenan hasta que el certificado expira o es revocado. Los registros relativos a las demás operativas se mantienen por tres (3) años.

Los certificados emitidos por la ACRN son mantenidos en su directorio público por tiempo indefinido, incluso luego de su expiración y/o revocación, para permitir a terceros validar las firmas que fueron realizadas con ellos.

5.6 – Cambio de Claves

No se realiza cambio de claves de certificados en la ACRN.

5.7 – Continuidad de Operaciones

La ACRN tiene definidos planes de continuidad del negocio y recuperación ante desastres, que le permiten continuar con su operativa en la eventualidad de fallas de equipamiento y/o siniestros. Estos planes contienen un análisis de riesgos de interrupción del servicio y las estrategias de recuperación propuestas, así como también las ventanas máximas de interrupción aceptables.

Los servicios de publicación de CRL y certificados emitidos por la ACRN están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de la AGESIC, ésta dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

Los pedidos de revocación son atendidos en un máximo de 24 horas.

5.7 – Terminación de las Operaciones

Los procedimientos de terminación de las operaciones se especifican en el punto 4.11.

6 – Controles de Seguridad Técnica

Los controles técnicos descriptos en esta sección tienen el objetivo de proteger el par de llaves de la ACRN 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 del sistema de CA de la ACRN se realiza 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

Estipulado en la Política de Certificación de la ACRN.

6.2 – Generación e Instalación de pares de llaves

6.2.1 – Autoridad Certificadora Raíz Nacional

El par de llaves de la ACRN es 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, según la presente CPS y de acuerdo a lo estipulado en el Guión de la Ceremonia de Claves.

6.2.2 – Autoridad Certificadora del Prestador Acreditado

El PSCA deberá elaborar un guión detallado de las actividades a realizar para poner en marcha su ACPA, incluyendo la generación de llaves, y deberá realizar la instalación en forma auditada y de acuerdo a dicho guión. Este deberá cubrir todo el proceso de instalación: sistema operativo, aplicaciones de CA, configuración de las aplicaciones,

generación y respaldo de llaves, generación del CSR, instalación del certificado de la ACPA (luego de emitido por la ACRN) y puesta en funcionamiento final de las funcionalidades de gestión de certificados y servicios de estado (CRL u OCSP).

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

6.3 – Protección de llave privada y controles de Módulos Criptográficos

Se cumple con lo estipulado en la Política de Certificación de la ACRN.

La ACRN publica su clave pública en su repositorio de información como parte del certificado.

La protección de la clave privada se realiza en un módulo HSM que cumple con la normativa estipulada en la Política de Certificación de la ACRN.

La llave privada de la ACRN se encuentra siempre dentro del HSM. El equipamiento de producción y el de contingencia tiene los controles de seguridad físicos y lógicos requeridos por la Política de Certificación de la ACRN y la presente Declaración de Prácticas de Certificación.

El retiro de la llave privada de los HSM se realiza únicamente para procedimientos de respaldo de la llave en otro HSM, procedimientos de *escrow* y para el cambio de HSM, en cuyos casos se retira en forma cifrada. Estos procedimientos son aprobados y controlados por la UCE.

Una vez que el certificado de la ACRN expira, se procede a la destrucción de la clave privada. La destrucción se realiza con un mecanismo que impide su recuperación. El HSM utilizado provee funciones para la eliminación segura de la llave privada.

6.4 – Otros aspectos de gestión de llaves

La ACRN mantiene un archivo de todos los certificados que contienen claves públicas utilizadas para la emisión de certificados, es decir, todos los certificados alguna vez utilizados como certificados de ACRN. De esta forma, es posible validar las cadenas de confianza de PKI Uruguay para cualquier instante de tiempo.

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

El período máximo de validez del par de llaves de la ACRN 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 es eliminada (ver 6.2 – Protección de la llave privada y controles de Módulos Criptográficos).

6.5 – Datos de activación

La ACRN entiende los procesos de activación y desactivación de llave privada de acuerdo a la definición dada para ellos en la Política de Certificación de la ACRN.

Para la activación de las llaves privadas de la ACRN se requiere la participación de varios individuos (custodios) en un esquema "M de N". Esta división del conocimiento impide que un individuo por sí solo tenga el conocimiento suficiente para activar la llave privada. Para la ACRN M es igual a tres y N es igual a ocho.

En la ACRN la llave privada se activa al iniciar el sistema para emitir una CRL o un certificado. La desactivación se realiza tras la emisión de la CRL o del certificado.

Los datos para la activación de la llave privada de la ACRN son *tokens*, algunos de ellos además complementados con un PIN.

6.6 – Seguridad computacional

La ACRN implementa políticas, estándares y procedimientos que permiten una operación segura.

Se instrumentan 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 son objeto de regulación por parte de la UCE.

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

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

Estos controles son objeto de regulación por parte de la UCE.

6.8 – Seguridad de la red

La ACRN opera en modalidad offline, por lo que no está conectada a ninguna red.

6.9 – Sincronización Horaria

La ACRN utiliza la fecha y hora de la República Oriental del Uruguay al firmar los certificados que emite, con un margen de error máximo del orden del minuto.

Durante la Ceremonia de Claves se establece esta hora y es certificada ante escribano público. La sincronización horaria es objeto de control de las auditorías periódicas.

7 – Perfil de certificados y de Listas de certificados revocados

7.1 – Perfil del Certificado de la ACRN

Estipulado en la Política de Certificación de la ACRN.

7.2 – Perfil del Certificado de las ACPA

Estipulado en la Política de Certificación de la ACRN.

7.3 – Perfil de la CRL de la ACRN

Estipulado en la Política de Certificación de la ACRN.

8 – Administración Documental

8.1 – Procedimiento para cambio de especificaciones

La ACRN cuenta con procedimientos internos para la administración de los cambios sobre la presente Declaración de Prácticas de Certificación.

8.2 – Procedimientos de Publicación y Notificación

Se publican en el sitio web de la ACRN las modificaciones aprobadas a la presente Declaración de Prácticas de Certificación, indicando en cada caso las secciones y/o textos reemplazados junto con la publicación de la nueva versión. Además, se publica 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 son notificados directamente ante cualquier cambio en estos términos o en la presente Declaración de Prácticas de Certificación.