CORREO URUGUAYO

Administración Nacional de Correos del Uruguay

Unidad de Servicios Electrónicos

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

OID 2.16.858.10000157.66565.6

Versión: 1.4

Abril de 2019

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.

En este contexto, la Administración Nacional de Correos (ANC) es un PSCA dentro de la cadena de confianza de la PKI Uruguay.

La presente Declaración de Prácticas de Certificación contiene las prácticas empleadas por la Administración Nacional de Correos (ANC) en su autoridad de certificación para la gestión de certificados y CRL.

1.2 IDENTIFICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Nombre: Declaración de Prácticas de Certificación

Versión: 1.0

Fecha de elaboración: marzo 2013

OID: 2.16.858.10000157.66565.6

Sitio web de publicación: ancca.correo.com.uy/ancca/cps.pdf

1.3 ENTIDADES Y PERSONAS INTERVINIENTES

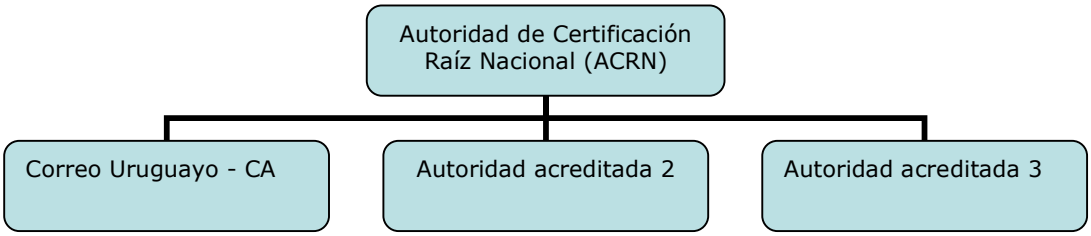
1.3.1 Unidad Reguladora

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. La ACRN es el certificado de nivel más alto en la jerarquía de PKI Uruguay.

La Autoridad de Certificación (Correo Uruguayo - CA) de la Unidad de Servicios Electrónicos de la ANC está en el siguiente nivel en la jerarquía de PKI Uruguay y es la entidad encargada de la firma de los certificados emitidos a entidades finales y de las listas de revocación.



- Un primer nivel en el que se ubica la ACRN representa el punto de confianza de todo el sistema;
- Un segundo nivel, constituido por las CA acreditadas por la ACRN que emitirán los certificados de entidad final;
- La ACRN podrá tener varias autoridades acreditadas.

1.3.3 Autoridad de Registro

La Autoridad de Registro (RA) es parte integrante de los Servicios de Certificación de la ANC. Funciona en los denominados "Puntos de Emisión" de certificados y tienen como misión realizar las funciones de identificación, registro y validación.

Podrá ser punto de emisión cualquier lugar acondicionado para dicho fin y con personal entrenado y autorizado de la ANC.

1.3.4 Suscriptores

Se entiende como usuario suscriptor a cualquier persona o sistema que voluntariamente confíe y haga uso de un certificado emitido por los Servicios de Certificación de la ANC.

Es obligación de todo usuario suscriptor el conocimiento de las condiciones y limitaciones expresadas en esta CPS.

1.3.5 Terceros aceptantes

Los Terceros Aceptantes son todas las personas o entidades diferentes del titular que deciden aceptar y confiar en un certificado emitido por los Servicios de Certificación de la ANC.

1.4 USO DE LOS CERTIFICADOS

1.4.1 Usos permitidos de los certificados

Los usos permitidos de los certificados serán exclusivamente los descriptos en las Políticas de Certificación asociadas a cada tipo de certificado, publicadas y mantenidas por la UCE.

La página de publicación de estas políticas es:
http://uce.gub.uy/informacion-tecnica/politicas/

1.4.2 Limitaciones y restricciones en el uso de los certificados

Los certificados deben emplearse únicamente de acuerdo con la legislación que le sea aplicable.

Los certificados no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

1.5 ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

1.5.1 Correo Uruguayo como responsable de la CPS

La Administración de la presente Declaración de Prácticas de Certificación es responsabilidad de la Unidad de Servicios Electrónicos de la ANC.

Por consultas o sugerencias, ANC designa al siguiente contacto:

Nombre: Unidad de Servicios Electrónicos
Dirección de correo: sel@correo.com.uy
Teléfono: (+598) 2916 0200

1.5.2 Procedimientos de aprobación de esta CPS

Esta CPS será revisada y aprobada por la UCE según la normativa aplicable vigente.

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 Definiciones

En el ámbito de esta CPS se utilizan las siguientes denominaciones:

Autenticación: procedimiento de comprobación de la identidad de una persona o entidad.

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.

Certificado reconocido: certificado expedido por un Prestador de Servicios de Certificación Acreditado que cumple los requisitos establecidos en la Ley.

Clave de Sesión: clave que se establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, sesión, terminando su utilidad una vez finalizada ésta.

Clave Personal de Acceso (PIN): secuencia de caracteres conocidos únicamente por el titular que permiten el acceso a los certificados.

Clave Pública y Clave Privada: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas solo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Directorio: repositorio de información que sigue el estándar X.500 de ITU-T.

Dispositivo criptográfico: instrumento que sirve para generar y almacenar los certificados tal que la generación y utilización del mismo se produzcan dentro del dispositivo y bajo la protección de un PIN.

Firma digital: nombre comercial de los tipos de certificados que maneja la CA.

Firma electrónica: conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

Función hash: operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible deducir otros mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados.

Identificador: conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

Jerarquía de confianza: conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior.

Listas de Revocación de Certificados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

Módulo Criptográfico: módulo de hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

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.

Solicitante: persona que solicita un certificado para sí mismo o para una entidad que le pertenece

Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado de un tercero.

Titular: persona o entidad para el que se expide un certificado

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.

1.6.2 Acrónimos

ACRN: Autoridad Certificadora Raíz Nacional.
AGESIC: Agencia para el desarrollo del Gobierno de gestión Electrónica y la Sociedad de la Información y del Conocimiento.
ANC: Administración Nacional de Correos o Correo Uruguayo.
ARL: Authority Revocation List (Lista de Autoridades Revocadas).
C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CA: Autoridad de Certificación.
CEN: Comité Européen de Normalisation (Comité Europeo de Normalización).
CI: Cédula de Identidad.

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
CP: Políticas de Certificación. En el ámbito de PKI Uruguay, estas son publicadas y mantenidas por la UCE.
CPS: Certificate Practice Statement (Declaración de Prácticas de Certificación).
CRL: Certificate Revocation List (Lista de Certificados Revocados).
CWA: CEN Workshop Agreement.
DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
E: Email (Correo electrónico). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
FIPS: Federal Information Processing Standard (Estándares del Gobierno Norteamericano para el procesamiento de la información).
HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.
IETF: Internet Engineering Task Force (Organismo de estandarización de Internet).
O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.
OID: Object identifier (Identificador de objeto único).
OU: Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
PKI: Public Key Infrastructure (Infraestructura de Clave Pública).
PKIX: Grupo de trabajo del IETF (Public Key Infrastructure X509 IEFT WorkingGroup) constituido con el objeto de desarrollar las especificación relacionadas con las PKI e Internet.
PSCA: Prestador de Servicios de Certificación Acreditado.
RA: Autoridad de Registro.
RFC: Request For Comments (Estándar emitido por la IETF).
S: State (Estado). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
UCE: Unidad de Certificación Electrónica.

2 REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

Se puede navegar en el sitio web de ANC por toda la documentación de información relacionada a la CA e instructivos para clientes. La información contenida en los repositorios de información no es de carácter confidencial. Los enlaces directos a la información relacionada con la PKI se adjuntan a continuación.

Certificado de la ACRN

http://www.uce.gub.uy/acrn/acrn.cer

Certificado del PSCA

http://ancca.correo.com.uy/ancca/ancca.cer

Lista de Certificados revocados (CRL)

http://ancca.correo.com.uy/ancca/ancca.crl

Servicio OCSP

http://ancca.correo.com.uy/ancca/OCSP

Ubicación de la CPS

http://ancca.correo.com.uy/ancca/cps.pdf

Ubicación de las CPs

http://uce.gub.uy/informacion-tecnica/politicas/

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El contenido de esta CPS, junto con cualquier otra información que se publique estará ubicada en la página http://www.correo.com.uy/

Cualquier persona que lo solicite podrá obtener una impresión de la CPS firmada por cualquiera de las autoridades responsables de la misma solicitándola por cualquier vía de contacto disponible en esta CPS.

Cualquier modificación a esta CPS será informada a la UCE y publicada en el repositorio declarado anteriormente.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

Para el certificado de la CA

La publicación del certificado de la ANC se llevará a cabo con anterioridad al comienzo de la prestación del servicio a través de la página oficial de ANC.

Para la lista de certificados revocados (CRL)

La CA publicará los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en la política de certificación de cada tipo de certificado.

Para la CPS

La publicación de la CPS se llevará a cabo con anterioridad al comienzo de la prestación del servicio y se mantendrá en vigencia hasta la publicación de una nueva CPS.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la lectura a los repositorios antes mencionados (certificados de CA, CRLs, CPS y Políticas) es abierto y público, pero solo personal autorizado podrá

modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello, ANC establecerá mecanismos que impidan a personas no autorizadas manipular la información contenida en los repositorios.

3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

3.1 NOMBRES

3.1.1 Tipos de nombres

Los certificados emitidos por ANC contienen el nombre distintivo (*distinguished name* o DN) X.500 del emisor y el destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

El DN del emisor tiene los siguientes campos y valores fijos:

CN = Correo Uruguayo - CA
O = ADMINISTRACIÓN NACIONAL DE CORREOS
C = UY

En el DN de la entidad solicitante se incluyen los campos definidos en la política de certificación de cada tipo de certificado.

3.1.2 Necesidad de que los nombres sean significativos

Para todos los tipos de certificados se garantiza que el nombre distintivo (DN) es suficientemente significativo para vincular la clave pública con una entidad.

3.1.3 Reglas para interpretar varios formatos de nombres

La regla utilizada por ANC para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4 Unicidad de los nombres

Para todos los tipos de certificados se garantiza que el nombre distintivo (DN) es suficientemente significativo para vincular una clave pública con una única entidad. Pueden existir dos certificados válidos con el mismo DN concurrentemente, pero estos certificados identificarán siempre a una misma entidad.

3.1.5 Reconocimiento, autenticación y papel de las marcas registradas

El proceso de presentar la documentación en el momento de la solicitud de un certificado asegura la utilización legítima y el permiso explícito para la utilización de toda denominación o marca registrada en la validación y emisión de un certificado.

3.2 VALIDACIÓN DE LA IDENTIDAD INICIAL

3.2.1 Medio de prueba de posesión de la clave privada

En el proceso de solicitud, el solicitante sigue las indicaciones de la página web desarrollada por la ANC que lo guían durante todo el proceso, utilizando el sistema web o descargando una aplicación desarrollada para dicho fin. Este método garantiza que la generación de claves se hace de acuerdo a los algoritmos, largo de clave y otras características definidas por la política de certificación asociada a cada tipo de certificado.

Luego de generadas las claves, el sistema se comunica con los servidores de la ANC de forma segura a través de SSL y utilizando una clave única del sistema donde se envían los datos del solicitante y la solicitud PKCS#10.

Finalmente al solicitante se lo dirige a la página, donde imprime un formulario con código de barras único asociado a su solicitud con el cual debe presentarse en un punto de emisión.

3.2.2 Autenticación de la identidad de una persona jurídica

La persona física que representa a la persona jurídica deberá demostrar en primera instancia su propia identidad presentando el documento de identidad correspondiente, vigente y en buen estado.

Luego de eso, deberá demostrar nombre y número de registro de la persona jurídica y su representación, presentando certificado notarial que lo acredita, con no más de 30 días desde su emisión.

3.2.3 Autenticación de la identidad de una persona física

El solicitante debe presentar documento de identidad vigente y en buenas condiciones. Este documento de identidad puede ser la cédula de identidad uruguaya o, en caso de ser extranjero, el pasaporte.

3.2.4 Información no verificada sobre el solicitante

Se verifica toda la información de acuerdo a la política de certificación de cada tipo de certificado.

3.2.5 Comprobación de las facultades de representación

Siempre que se requiera comprobar representación se solicitará un certificado notarial que lo acredite, con no más de 30 días desde su emisión.

3.2.6 Criterios para operar con CAs externas

No se opera con CAs externas.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN EN LAS PETICIONES DE RENOVACIÓN DE CLAVES Y CERTIFICADOS

3.3.1 Identificación y autenticación por una renovación de claves de rutina

El procedimiento de renovación en todos los casos es exactamente el mismo que el procedimiento de emisión por primera vez, por lo tanto, no hay consideraciones especiales.

En el caso de que hubiera un procedimiento de renovación diferente, se haría de acuerdo a la política de certificación de cada tipo de certificado.

3.3.2 Identificación y autenticación para una renovación de claves tras una revocación

El procedimiento de renovación en este caso es exactamente el mismo que el procedimiento de emisión por primera vez, por lo tanto, no hay consideraciones especiales.

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Quién puede efectuar una solicitud

Definido de acuerdo a la política de certificación de cada tipo de certificado.

4.1.2 Registro de las solicitudes de certificados

En el proceso de solicitud, el solicitante utiliza un sistema desarrollado por la ANC que lo guía durante todo el proceso. Este método garantiza que el procedimiento de solicitud se hace de acuerdo a los algoritmos, largo de clave y otras características definidas por la política de certificación asociada a cada tipo de certificado.

Si la política define que la clave privada debe ser generada en un dispositivo seguro de creación de firma (DSCF) por hardware, el sistema utiliza una librería nativa de los dispositivos para solicitar la generación de claves. De este modo la ANC garantiza que las claves se generan dentro de un DSCF homologado por ANC.

Si la política define que la clave privada debe ser generada en un dispositivo o módulo seguro de creación de firma (DSCF) por hardware o software, se permite la generación de las claves fuera del sistema y el ingreso de una solicitud PKCS#10.

Luego de generadas las claves, la aplicación se comunica con los servidores de la ANC de forma segura a través de SSL donde se envían los datos del solicitante y la solicitud PKCS#10.

Finalmente, al solicitante se lo dirige a la página donde imprime un formulario con código de barras único asociado a su solicitud con el cual debe presentarse en un punto de emisión.

4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación son realizadas en todos los casos por funcionarios de ANC, quienes validan la información en presencia del titular y su documento de identidad. Estos funcionarios están debidamente capacitados para el correcto desempeño de esta tarea.

4.2.2 Aprobación o denegación de las solicitudes de certificados

El personal de la CA aprobará y emitirá los certificados digitales solo en el caso que se hayan seguido los Procedimientos de Emisión correspondientes a cada tipo de certificado.

Si por algún motivo, el funcionario que realiza la identificación y autenticación o bien el personal de la CA que aprueba los certificados sospecha o constata que hubo alguna anomalía en la información presentada o una falta a los procedimientos definidos, no se emitirá el certificado.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

El plazo entre el registro de solicitud de un certificado (dado por la validación presencial de la identidad del Solicitante) y la entrega del certificado será de 24 horas en la Casa Central y de 72 horas en cualquier otro caso.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 Actuaciones de la CA durante la emisión de los certificados

El personal de la CA, luego de corroborar que todos los Procedimientos de Emisión fueron realizados correctamente, admite la realización del certificado. Este certificado se genera utilizando un procedimiento que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

En todo momento se protege la confidencialidad e integridad de los datos de registro cifrando a través de SSL toda información que viaja entre la RA y la CA. La CA genera el certificado y lo devuelve a la RA para su posterior notificación al solicitante de la emisión de su certificado.

Todas las actuaciones de la CA quedan registradas en una bitácora disponible para aquellos auditores del sistema de la CA designados para dicho fin.

4.3.2 Notificación al solicitante de la emisión por la CA del certificado

La CA notifica al solicitante de la emisión de su certificado a través del correo electrónico seleccionado para dicho fin por el solicitante. Éste puede instalar el certificado siguiendo las instrucciones que acompañan el correo de acuerdo a cada tipo de certificado.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 Forma en la que se acepta el certificado

La solicitud de certificados es de carácter voluntario y cualquier persona puede solicitar la revocación de su certificado de forma gratuita.

Si el usuario no manifiesta la intención de revocar dichos certificados tras la expedición, se dará por confirmada la aceptación de los mismos, así como de sus condiciones de uso.

El usuario tendrá hasta 1 mes corrido a partir de su emisión para realizar cualquier reclamación sobre su certificado o sobre cualquier condición que no considere adecuada y podrá solicitar una reemisión de su certificado sin costo. Luego de transcurrido un mes, el certificado se dará como aceptado completamente y no podrá ser reclamado.

4.4.2 Publicación del certificado por la CA

No aplica, ya que los certificados emitidos no se publicarán en ningún repositorio de acceso libre.

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

Solo cuando el titular así lo indique dando su expreso consentimiento la CA podrá notificar de la emisión de un certificado a otra entidad para facilitar su uso.

4.5 PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1 Uso de la clave privada y del certificado por el titular

El titular solo puede utilizar la clave privada y el certificado para los usos autorizados en esta CPS y de acuerdo a lo establecido en las Políticas de Certificación correspondiente. Esta Política de certificación es publicada y mantenida por la UCE.

Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en esta CPS y acorde a la normativa vigente.

Tras la extinción de la vigencia o la revocación del certificado el titular deberá dejar de usar la clave privada asociada para todo uso. Pese a que es recomendable que se acceda a todos los datos cifrados antes del vencimiento para re-cifrarlo con un nuevo certificado vigente, se permite el uso de estas claves para el acceso a datos que pudieran estar cifrados para re-cifrarlos con un nuevo certificado.

4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes

Los Terceros Aceptantes solo pueden depositar su confianza en los certificados para aquello que establece esta CPS y de acuerdo con lo establecido en las Políticas de Certificación correspondientes publicadas y mantenidas por la UCE.

Los Terceros Aceptantes han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta CPS. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos y en la normativa vigente.

4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

No aplica, ya que todas las renovaciones de certificados realizadas en el ámbito de esta CPS se realizarán con cambio de claves.

4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

4.7.1 Circunstancias para una renovación con cambio claves de un certificado

El procedimiento de renovación es exactamente el mismo que el procedimiento de emisión por primera vez pudiéndose utilizar el mismo dispositivo para el certificado siempre y cuando este dispositivo siga estando homologado por la CA.

4.7.2 Quién puede pedir la renovación de un certificado

El proceso de renovación de los certificados deberá ser solicitado de forma voluntaria y por iniciativa del solicitante. Éste deberá realizar la solicitud del mismo modo que lo haría para un certificado nuevo o de acuerdo a la política de certificación de cada tipo de certificado.

4.7.3 Tramitación de las peticiones de renovación con cambio de claves

El procedimiento de tramitación es exactamente el mismo que el procedimiento de tramitación por primera vez.

4.7.4 Notificación de la emisión de nuevos certificado al titular

El procedimiento de notificación es exactamente el mismo que el procedimiento de notificación por primera vez.

4.7.5 Forma de aceptación del certificado con nuevas claves

Las consideraciones de la forma de aceptación son exactamente las mismas que las de la primera vez.

4.7.6 Publicación del certificado con las nuevas claves por la CA

No aplica, ya que los certificados emitidos no se publicarán en ningún repositorio de acceso libre.

4.7.7 Notificación de la emisión del certificado por la CA a otras Autoridades

Solo cuando el titular así lo indique dando su expreso consentimiento la CA podrá notificar de la emisión de un certificado a otra entidad para facilitar su uso.

4.8 MODIFICACIÓN DE CERTIFICADOS

4.8.1 Causas para la modificación de un certificado

No se realizan modificaciones a un certificado por ninguna causa. El solicitante podrá solicitar una revocación de su certificado y la tramitación de un nuevo certificado siguiendo los procedimientos antes mencionados.

Si esta revocación y su nueva solicitud se realizan en un plazo menor a un mes corrido a partir de su emisión original, el certificado nuevo será sin costo.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación y suspensión de los certificados son mecanismos a utilizar en el supuesto de que por alguna causa se deje de confiar en dichos certificados antes de la finalización del período de validez originalmente previsto.

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su fecha de caducidad. El efecto de la revocación de un certificado es la pérdida de validez del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, la revocación de un certificado inhabilita el uso legítimo del mismo por parte del titular.

4.9.1 Causas para la revocación

Las causas para la revocación de los certificados se especifican en la Política de Certificación correspondiente a cada tipo de certificado.

4.9.2 Quién puede solicitar la revocación

La información de la habilitación para solicitar la revocación se especifica en la Política de Certificación correspondiente a cada tipo de certificado.

4.9.3 Procedimiento de solicitud de revocación

De acuerdo a la política de certificación de cada tipo de certificado la revocación puede admitir varias formas: presencial, remota, auto-revocación o por un tercero.

4.9.3.1 Solicitud Presencial

En este caso, se requiere la presencia física del interesado en uno de los puntos de emisión. La documentación a presentar se especifica en la Política de Certificación correspondiente a cada tipo de certificado.

Procedimiento:

1- El interesado se presenta en uno de los puntos de revocación.

2- El Operario pregunta al interesado cuál es la razón para la revocación.

3- El Operario verifica que la documentación presentada por el interesado sea correcta.

4- El Operario informa al interesado que el proceso de revocación es irreversible y que implica la pérdida definitiva del certificado.

5- El Operario aprueba la solicitud de revocación e informa al personal de la CA.

6- Personal de la CA revoca el certificado y se publica una nueva crl.

4.9.3.2 Solicitud Remota

En este caso, el titular solicita la revocación de su certificado a través de la página del Correo Uruguayo, ingresando información de su conocimiento.

Procedimiento:

1- El interesado ingresa a la página del Correo Uruguayo y navega hasta la página de revocación.

2- La página informa al interesado que el proceso de revocación es irreversible y que implica la pérdida definitiva del certificado.

3- El solicitante ingresa el motivo, número único de su certificado, su número de documento de identidad y selecciona revocar.

4- Personal de la CA recibe y verifica la solicitud de revocación.

5- Personal de la CA revoca el certificado y se publica una nueva crl.

4.9.3.3 Auto-Revocación

En este caso, el titular solicita la revocación de su certificado a través de la página del Correo Uruguayo, ingresando información de su conocimiento y autenticándose mediante su certificado.

Procedimiento:

1- El interesado ingresa a la página del Correo Uruguayo y navega hasta la página de revocación automática.

2- La página informa al interesado que el proceso de revocación es irreversible y que implica la pérdida definitiva del certificado.

3- El solicitante ingresa el motivo, número único de su certificado y selecciona revocar.

4- La CA revoca el certificado y se publica una nueva crl.

4.9.3.4 Por un tercero

En el caso que la política lo requiera, un tercero podrá solicitar la revocación de un certificado a través de un servicio diseñado para dicho fin.

4.9.4 Plazo en el que la CA debe resolver la solicitud de revocación

Para la revocación de un certificado puede transcurrir, entre el registro de la solicitud y la publicación de la nueva CRL (con el certificado revocado), un plazo máximo de 12 horas.

4.9.5 Requisitos de verificación de las revocaciones por los terceros aceptantes

El procedimiento ordinario de comprobación de la validez de un certificado será la verificación contra la CRL publicada. Opcionalmente los terceros podrán validar la revocación contra el servicio OCSP.

4.9.6 Frecuencia de emisión de CRLs

La CA emitirá una nueva CRL cada 24 horas. La validez de esta CRL será de 48 horas.

4.9.7 Tiempo máximo entre la generación y la publicación de las CRL

La CA genera y publica la CRL en un mismo proceso, por lo tanto no existe un tiempo entre generación y publicación.

4.9.8 Disponibilidad de un sistema en línea de verificación del estado de los certificados (OCSP)

ANC cuenta con un servicio de validación de estado de certificados OCSP.

El servicio está publicado en la dirección http://ancca.correo.com.uy/ancca/OCSP

4.9.9 Requisitos de comprobación en línea de revocación

Los terceros deberán contar con las herramientas necesarias para consumir el servicio OCSP publicado por la ANC.

4.9.10 Otras formas de divulgación de información de revocación disponibles

No existen otras formas de divulgación.

4.9.11 Requisitos especiales de renovación de claves comprometidas

No existe renovación de claves comprometidas.

4.9.12 Circunstancias para la suspensión

No se suspenden certificados.

4.9.13 Quién puede solicitar la suspensión

No aplica.

4.9.14 Procedimiento para la solicitud de suspensión

No aplica.

4.9.15 Límites del periodo de suspensión

No aplica.

4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1 Características operativas

La CRL se encuentra accesible, en formato X.509 v2, en la siguiente URL: http://ancca.correo.com.uy/ancca/ancca.crl.

Esta dirección puede estar presentes en la extensión "cRLDistributionPoints" en cada certificado emitido de acuerdo a las Políticas de Certificación de cada tipo de certificado.

El servicio OCSP para validación online se encuentra accesible en la siguiente URL: http://ancca.correo.com.uy/ancca/OCSP

4.10.2 Disponibilidad del servicio

Tanto la CRL como el servicio OCSP están disponibles de forma ininterrumpida todos los días del año.

4.10.3 Características adicionales

No aplica.

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

El fin de la suscripción ocurre en las siguientes situaciones:

- El certificado alcanzó su fecha de expiración;
- El certificado fue revocado;
- El certificado del Correo Uruguayo fue revocado por la ACRN.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 Prácticas y políticas de custodia y recuperación de claves

No se realiza custodia de claves ni tampoco recuperación de claves. Para todos los casos de clave comprometida se deberá revocar el certificado y emitir un nuevo certificado.

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión

No aplica.

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y OPERACIONALES

En la presente sección se describirá el entorno de seguridad física en el que se encuentran enmarcados los servicios de certificación de la ANC. En particular y entre otros, se detallarán los controles de los servicios de certificación, la seguridad física de la oficina central y los controles sobre el personal.

5.1 CONTROLES DE SEGURIDAD FÍSICA

5.1.1 Ubicación física y construcción

La CA del Correo Uruguayo se encuentra ubicada en un datacenter Tier 3.

5.1.2 Acceso físico

Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Para el acceso las instalaciones de la CA de la ANC se mantienen los siguientes criterios:

- Se obtiene la protección física definiendo un claro perímetro de seguridad englobando el lugar físico de la CA;
- Este perímetro está sellado, no tiene ventanas ni puertas traseras;
- Se mantienen barreras de seguridad para prevenir accesos no autorizados;
- Las puertas de acceso al lugar físico de la CA tienen alarmas y están cerradas;
- El lugar físico de la CA queda protegido con alarma cuando nadie lo ocupa;
- El lugar físico de la CA queda trancado;
- No está permitido el trabajo de personal externo a la CA no supervisado;
- El acceso al lugar físico de la CA se debe hacer mediante un proceso de identificación;
- Los visitantes permitidos dentro de la CA deben ser supervisados y se debe registrar su entrada.

5.1.3 Alimentación eléctrica y aire acondicionado

El datacenter donde se ubican los equipos de la CA del Correo Uruguayo disponen de suministro de electricidad redundante e independiente y aire acondicionado adecuado a los requisitos de los equipos instalados. La infraestructura está protegida contra caídas de tensión o cualquier anomalía en el suministro eléctrico.

Las instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. El apagado de los equipos solo se producirá en caso de períodos prolongados de falta de suministro de energía eléctrica.

5.1.4 Exposición al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado.

5.1.5 Protección y prevención de incendios

El datacenter cuenta con medios adecuados de prevención, detección y extinción de incendios.

El cableado se encuentra en falso suelo de materiales ignífugos y la sala está equipada con un sistema de control de temperatura y un sistema de detección de humo.

5.1.6 Sistema de almacenamiento

La CA de ANC ha establecido los procedimientos necesarios para asegurar el almacenamiento de información seguro y con el respaldo adecuado.

Se cuenta con redundancia de toda la infraestructura y contingencia fuera de las instalaciones.

5.1.7 Eliminación de los soportes de información

La eliminación de soportes, tanto papel como magnéticos, se realiza mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

5.1.8 Copias de seguridad fuera de las instalaciones

Se replica toda la información crítica a equipos de respaldo fuera de las instalaciones con medidas de protección equivalentes.

5.2 CONTROLES DE PROCEDIMIENTO

5.2.1 Roles responsables del control y gestión de la PKI

Se distinguen los siguientes roles para la operación y gestión del sistema:

• **Custodios HSM (Modulo Seguridad Hardware)**: encargados de la definición de claves de administración del HSM, de su custodia, de su configuración y puesta en marcha;

• **Auditores**: autorizados a consultar archivos, trazas y logs de auditoría de las entidades de la PKI y auditar la documentación o procesos de la CA;

• **Validadores de Identidad RA**: funcionarios del Correo Uruguayo encargados de la validación de la identidad presencial de las entidades finales. Los funcionarios y personal contratado responsable de un puesto de expedición desempeñarán el rol de validadores;

• **Operadores de RA**: responsables de emitir y revocar los certificados. Serán los que revisarán que todas las validaciones se hayan cumplido correctamente, que toda la información esté completa y de acuerdo a los requerimientos y emitirán los certificados;

• **Operadores de CA**: encargados de la configuración y administración del software de PKI. Este rol es responsable de la configuración general del software de PKI, que incluye, entre otros, las configuraciones de acceso a las bases de datos, la configuración de los dispositivos criptográficos a utilizar para la autenticación ante el sistema y los directorios de trabajo del sistema;

• **Soporte Técnico**: conjunto de usuarios autorizados a realizar ciertas tareas relacionadas con la instalación, configuración y mantenimiento de las aplicaciones soporte de los sistemas PKI. Responsable del funcionamiento de los sistemas de hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de datos, del repositorio de información y de los sistemas operativos. Encargados también de ejecutar los procedimientos de backup y recuperación a este nivel.

5.2.2 Número de personas requeridas por tarea

Se requiere una de tres personas para realizar cualquier tarea que requiera activar el HSM.

5.2.3 Identificación y autenticación para cada usuario

Los Custodios HSM se identifican y autentican en los HSM mediante dispositivos específicos de los HSM.
El resto de roles autorizados a ingresar al sistema de PKI se identifican mediante certificados electrónicos y se autentican por medio de dispositivos criptográficos USB.

5.2.4 Roles que requieren segregación de funciones

Las tareas operativas de los Servicios de Certificación, (particularmente la emisión de certificados digitales) están segregadas de las tareas de auditoría de los sistemas vinculados.

Adicionalmente, las funciones de desarrollo y operación de los sistemas vinculados a los Servicios de Certificación están segregadas y garantizan que quienes introducen un cambio en un aplicativo/servicio no cuentan con el acceso para poner dicho cambio en producción sin pasar por el procedimiento de control de cambios.

5.3 CONTROLES DE PERSONAL

5.3.1 Requisitos relativos a la contratación, conocimiento y experiencia

Los Servicios de Certificación mantienen controles para asegurar que las prácticas de contratación de personal soportan y mejoran la confianza de las operaciones sobre la CA.

En la descripción del trabajo se establecen las responsabilidades tal como se especifican en las políticas de seguridad. Se realizan chequeos de verificación de personal a la hora de tomar nuevo personal permanente y estos firman un acuerdo de confidencialidad como parte de las condiciones iniciales de empleo. Todo personal de los Servicios de Certificación son funcionarios públicos.

El personal contratado pasa por un período no menor a 3 meses de capacitación y entrenamiento en las áreas referentes a la PKI antes de pertenecer a los roles de operadores de CA o Custodio.

5.3.2 Procedimientos de comprobación de antecedentes

Conforme a la normativa general de la Administración del Estado.

5.3.3 Requerimientos de formación

El personal relacionado con la administración de la PKI, recibirá la formación necesaria para asegurar la correcta realización de sus funciones.

Se incluyen en la formación los siguientes aspectos:

- Lectura completa de la Declaración de Prácticas y Políticas de Certificación;
- Lectura completa de la Política de Seguridad;
- Concienciación sobre la seguridad física, lógica y técnica;
- Procedimientos de seguridad;
- Procedimientos de operación;
- Procedimientos para la recuperación de la operación en caso de desastres.

5.3.4 Requerimientos y frecuencia de actualización de la formación

El proceso de actualización de formación es un proceso permanente donde el personal de la PKI se mantendrá al día con cursos o seminarios relacionados con los aspectos de la PKI.

No obstante, si hubiera una actualización o cambio en el software, o un cambio de hardware que amerite un curso especializado, la ANC contratará en sus propias oficinas un curso especializado para el personal de la PKI.

5.3.5 Frecuencia y secuencia de rotación de tareas

No se realiza rotación de tareas.

5.3.6 Sanciones por actuaciones no autorizadas

Un proceso disciplinario existe y se utiliza para empleados que hayan incumplido las políticas o procedimientos de seguridad. Estas irregularidades serán analizadas por las áreas competentes, acorde a la reglamentación del Estado y sancionadas, en su caso, por el Directorio de la ANC.

5.3.7 Requisitos de contratación de terceros

Se aplicara la normativa general de la ANC acorde a la reglamentación del Estado para la contratación de terceros.

5.3.8 Documentación proporcionada al personal

Se proporcionará la documentación de la normativa general de la ANC, así como también ésta CPS y las Políticas de Certificación asociadas.

5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.4.1 Tipos de eventos registrados

Se registrarán todos los eventos relacionados con la operación y gestión del sistema, así como los relacionados con la seguridad del mismo, entre otros:

- Arranque y parada de aplicaciones;
- Intentos exitosos o fracasados de inicio y fin de sesión;
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs;
- Cambios en la configuración del sistema;
- Mantenimiento del sistema;
- Cambios en las políticas de emisión de certificados;
- Registros de acceso físico de personal no perteneciente a la PKI.

5.4.2 Frecuencia de procesado de registros de auditoría

Los registros se analizan dependiendo de la criticidad de los eventos y pueden procesarse inmediatamente mediante alertas o manualmente con una frecuencia mensual o anual.

5.4.3 Período de conservación de los registros de auditoría

La información generada por los registros de auditoría se mantiene en línea y es accesible a través del sistema de PKI. Estos registros se mantendrán accesibles hasta el vencimiento de la CA.

5.4.4 Protección de los registros de auditoría

Los registros de auditoría están protegidos mediante técnicas criptográficas de forma que nadie, salvo las propias aplicaciones de visualización de eventos con su debido control de accesos, pueda acceder a ellos.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Estos registros están almacenados en las bases de datos y por lo tanto cuentan con todos los mecanismos de respaldo asociados a las mismas.

Las bases de datos se encuentran replicadas en equipos fuera de las instalaciones con características de seguridad equivalentes.

5.4.6 Sistema de recolección de información de auditoría

El sistema de recolección de auditoría está totalmente integrado con la aplicación de PKI.

5.4.7 Notificación al sujeto causa del evento

El sistema maneja varios informes de error que se muestran al usuario y generan registros de auditoría, pero no se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento. Será decisión de los auditores la notificación al operador o a las autoridades cuando ésta sea relevante.

5.4.8 Análisis de vulnerabilidades

Tanto el hardware como el software adquirido para el desarrollo de la PKI de ANC cumplen con los más altos estándares de seguridad del mundo. Estos estándares y criterios analizan profundamente los sistemas y el hardware contra vulnerabilidades.

De todos modos se realizan periódicamente análisis de vulnerabilidades de estos sistemas.

5.5 ARCHIVO DE REGISTROS

5.5.1 Tipo de registros archivados

La CA conserva toda la información concerniente a las operaciones realizadas con los certificados en línea hasta el vencimiento de la CA.

No existe un proceso de archivo de eventos, y terminado este período, toda la información se destruye siguiendo las reglas establecidas en el punto 5.1.7.

5.5.2 Periodo de conservación del archivo

Los registros se mantienen en línea y son accesibles a través del sistema de PKI. Estos registros se mantendrán accesibles hasta el vencimiento de la CA.

5.5.3 Protección del archivo

No aplica.

5.5.4 Procedimientos de respaldo del archivo

No aplica.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de PKI empleados por ANC garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas se sincroniza con el servidor de la CA.

5.5.6 Sistema de administración del archivo

No aplica, ya que la información de auditoría está siempre en línea.

5.5.7 Procedimientos para obtener y verificar información archivada

No aplica.

5.6 CAMBIO DE CLAVES DE UNA CA

No aplica.

5.7 RECUPERACIÓN EN CASOS DE COMPROMISO O CATÁSTROFE

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

Todo el personal de los Servicios de Certificación así como el resto del personal de la Administración Nacional de Correos que participa de alguna forma en los Servicios de Certificación está instruido en cómo detectar y reportar incidentes de seguridad a través de los canales definidos.

La respuesta ante cualquier incidente buscará en primera instancia la contención de dicho incidente para minimizar su impacto (incluyendo acciones de contingencia si corresponde), para luego pasar a un análisis detallado del incidente y sus causas tendiente a la preparación y ejecución de un plan de remediación. En cualquier caso, todo el ciclo de vida del incidente de seguridad será documentado formalmente como referencia futura y como justificación de las acciones que se hayan tomado en virtud del mismo. En particular, la documentación deberá reflejar todas las evidencias del incidente que se recaben, por si resultara deseable implementar acciones legales.

La ANC tiene establecidos mecanismos de redundancia y contingencia ante un posible acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación para recuperar las operaciones de la CA en un tiempo razonable.

Estos mecanismos, entre otros aspectos, cuentan con los siguientes componentes:

- La redundancia de los componentes más críticos;
- Equipos de respaldo alternativos;
- Procedimientos de respaldo diarios de todos los datos críticos;
- Acceso a los sistemas con autenticación por 2 factores.

5.7.2 Alteración de los recursos hardware, software y/o datos

La ANC tiene establecidos mecanismos de respaldos para recuperar las operaciones de la CA en un tiempo razonable, en caso de interrupción o falla de procesos críticos.

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

5.7.3 Procedimiento ante el compromiso de la clave privada de la CA

En el caso de que se viera afectada la seguridad de la clave privada de la CA, se procederá a su revocación comunicando a la UCE y siguiendo todos los procedimientos declarados en sus Políticas de Certificación.

5.7.4 Instalación después de un desastre natural u otro tipo de catástrofe

La CA puede ser reconstruida en caso de desastre (destrucción completa del datacenter) mediante el equipo de contingencia fuera de las instalaciones.

5.8 CESE DE UNA CA O RA

5.8.1 Autoridad de Certificación

La UCE, de acuerdo a sus Políticas de Certificación, o el Directorio de la ANC podrán poner fin a la actividad de la CA. En la circunstancia de que el Directorio de la ANC ponga un término a sus actividades, la CA dejará de emitir nuevos certificados pero se mantendrán todos los servicios de verificación de validez de los certificados emitidos hasta la fecha de vencimiento del último certificado de entidad final.

Al concretarse la terminación de sus actividades, la custodia de las claves quedará a cargo de personal de confianza de la ANC, durante el año en que se mantiene el servicio de publicación, para ser destruidas posteriormente.

5.8.2 Autoridad de Registro

No se cesará la actividad de una RA sin cese de actividades de la CA.

6 CONTROLES DE SEGURIDAD TÉCNICA

En la presente sección se describirá el entorno de seguridad técnica en el que se encuentran enmarcados los servicios de certificación de la ANC. En particular, y entre otros, se detallaran los controles de los servicios de certificación, la protección de las claves de la autoridad, seguridad informática y redes.

6.1 GENERACIÓN E INSTALACIÓN DE CLAVES

6.1.1 Generación del par de claves de la CA

Los pares de claves para la CA de ANC se generan en módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3.

El largo de clave de las claves de los Servicios de Certificación de la ANC es de 4096 bits y su certificado se encuentra publicado en el repositorio de la UCE.

Las claves de las entidades finales son generadas de acuerdo a lo definido en las Políticas de Certificación correspondientes publicadas y mantenidas por la UCE.

6.1.2 Entrega de la clave privada al titular

Para todos los casos, las claves son generadas por la entidad final y la forma de generación puede variar de acuerdo a lo definido en las Políticas de Certificación correspondientes publicadas y mantenidas por la UCE.

En todos los casos, las claves privadas de entidades finales están bajo su única posesión.

6.1.3 Entrega de la clave pública al emisor del certificado

El intercambio de la clave pública se hace de acuerdo a lo establecido en el punto 4.1.2.

6.1.4 Entrega de la clave pública de la CA a los terceros aceptantes

Las claves públicas de las Autoridades de Certificación Acreditadas están publicadas en el repositorio de la UCE.

Puede solicitarse la clave pública de la CA del Correo Uruguayo en la Casa Central de ANC.

6.1.5 Tamaño de las claves

El tamaño de las claves de la CA es de 4096 bits.

El tamaño de las claves de los certificados de entidad final será el definido en las Políticas de Certificación correspondientes, publicadas y mantenidas por la UCE.

6.1.6 Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de la CA está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA de 4096 bits.

El Hardware utilizado para la generación de las claves cumple con el estándar FIPS 140-1 Nivel 3 y cumple con todos los requerimientos de generación de claves de alta calidad.

6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para cada tipo de certificado emitido por ANC están definidos por la Política de Certificación que le sea aplicable.

6.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1 Estándares para los módulos criptográficos

Los HSM donde se encuentran las claves privadas de la CA Root y CA Subordinada, son módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3.

6.2.2 Control multipersona (m de n) de la clave privada

Se utiliza un control 1 de 3. Todos los mecanismos de acceso a la CA se realizan por autenticación doble (dispositivo y clave).

6.2.3 Custodia de la clave privada

La ANC no contrata a terceros para custodia de sus claves ni custodia claves de entidades finales.

6.2.4 Copia de seguridad de la clave privada

Las claves privadas de las CAs de la ANC están guardadas bajo la protección de los HSM que cada una de ellas posee. Las claves están respaldadas en otro HSM con las mismas características que el HSM donde se generaron.

6.2.5 Archivo de la clave privada

Las claves están respaldadas en otro HSM con las mismas características que el HSM donde se generaron.

6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico

La transferencia de la clave privada de las CAs de los servicios de certificación de la ANC solo se puede hacer entre módulos criptográficos (HSM).

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan directamente en el módulo criptográfico en el momento de la creación de la CA que hace uso de dichos módulos.

6.2.8 Método de activación de la clave privada

La clave privada de la CA, se activa mediante la inicialización del software de HSM utilizando dispositivos criptográficos. Posterior a la activación, la persona autorizada deberá autenticarse ante el sistema con su dispositivo con su respectiva clave (PIN). Éste es el único método de activación de la clave privada.

6.2.9 Método de desactivación de la clave privada

Un administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación de ANC mediante la detención del software de CA. Para su reactivación es necesario seguir el método expresando anteriormente.

6.2.10 Método de destrucción de la clave privada

En términos generales, la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.

En el caso de las CA de la ANC, la destrucción consistiría en el borrado seguro de las claves de los HSM que las albergase, así como de las copias de seguridad la misma. Para ello el HSM cuenta con herramientas diseñadas para dicho fin.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 Archivo de la clave pública

Los servicios de certificación de ANC mantendrán publicadas sus claves públicas hasta el vencimiento del último certificado de entidad final emitido por la correspondiente CA.

6.3.2 Períodos operativos de los certificados y período de uso para el par de claves

Los períodos de utilización de las claves son los determinados por la duración del certificado, y una vez transcurrido no se pueden seguir utilizando.

La caducidad producirá automáticamente la invalidación de los certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

Los certificados de entidad final tienen una validez de 1 o 2 años a partir de su emisión. La caducidad de un certificado de entidad final inhabilita el uso legítimo por parte de dicha entidad.

6.4 DATOS DE ACTIVACIÓN

6.4.1 Generación e instalación de los datos de activación

Para la generación de la Autoridad de Certificación de la ANC se crearon credenciales en dispositivos criptográficos, que servirán para actividades de administración, funcionamiento y recuperación. La CA opera con varios tipos de roles, cada uno con sus correspondientes dispositivos criptográficos donde se almacenan los datos de activación.

Para la activación del sistema de la Cas, es necesaria la intervención de los administradores del HSM que tienen el conocimiento de la contraseña o clave de acceso que permite activar las claves privadas. A su vez, los usuarios autorizados del sistema tendrán su dispositivo, con un PIN de acceso al sistema.

En el caso de las claves asociadas a los certificados de entidad final, el dato de activación consiste en el PIN o clave personal de acceso del dispositivo o almacén que las contiene.

6.4.2 Protección de los datos de activación

Solo el personal autorizado de la PKI de la ANC correspondientes a cada AC posee los dispositivos criptográficos y conoce las claves de acceso para acceder a los datos de activación.

En el caso de las claves asociadas a los certificados de entidad final, solo el titular conoce la clave de acceso o PIN, siendo por tanto el único responsable de la protección de los datos de activación de sus claves privadas. Esta responsabilidad está a su vez plasmada en un contrato en soporte papel que se firma entre la ANC y la entidad final donde el titular se compromete a su correcto resguardo.

6.4.3 Otros aspectos de los datos de activación

En todos los casos, las claves de acceso son de carácter confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados en los distintos sistemas; por lo tanto, debe seleccionarse a conciencia y tratarse con especial cuidado.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1 Requerimientos técnicos de seguridad específicos

El acceso a los sistemas de la CA está restringido a personal autorizado mediante controles de acceso de usuarios a los sistemas operativos y a las aplicaciones de PKI.

Existen políticas de control de acceso a los sistemas que incluyen:

- Roles con sus correspondientes permisos;
- Identificación y autenticación por usuario;
- Autenticación doble (dispositivo criptográfico y clave);
- Segregación de tareas.

Se sigue un proceso de registro y borrado de usuarios para permitir el acceso a los sistemas y la modificación de privilegios y el manejo de las claves de acceso de los mismos está restringida y controlada.

Se requiere a todos los usuarios del sistema que sigan procedimientos seguros en la elección y modificación de claves de acceso.

6.5.2 Evaluación de la seguridad informática

Al momento de selección del software de PKI a utilizar se realizó un exhaustivo análisis de los sistemas existentes evaluando especialmente las normas de seguridad que cumplían. El sistema de PKI de los Servicios de Certificación de la ANC cumple con los más altos estándares de seguridad.

Se mantienen controles anuales para asegurar que estos sistemas sigan cumpliendo con las normas y estándares.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.1 Controles de desarrollo de sistemas

Al momento de selección del software de PKI a utilizar, la ANC realizó un exhaustivo análisis de los sistemas existentes. El sistema de PKI adquirido de los servicios de certificación de la ANC cumple con el Common Criteria EAL 3+.

Los requerimientos de seguridad de cualquier aplicación involucrada en la provisión de los Servicios de Certificación están documentados formalmente y aprobados por el Responsable de la CA.

El acceso al código fuente de cualquiera de las aplicaciones involucradas en la provisión de los Servicios de Certificación está limitado exclusivamente al personal autorizado formalmente por el Responsable de la CA.

Toda modificación realizada sobre las aplicaciones involucradas en la provisión de los Servicios de Certificación es sometida a un procedimiento formal de prueba/validación.

6.6.2 Controles de gestión de seguridad

El correcto funcionamiento de los sistemas se chequea por personal calificado de forma periódica y se realizan pruebas de funcionamiento y un seguimiento de las necesidades de crecimiento.

Se han definido procedimientos periódicos de monitoreo y auditoría para verificar que todos los procesos de gestión de seguridad de la información se llevan adelante adecuadamente.

6.6.3 Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tienen impacto en la seguridad de ANC, por ejemplo, el análisis de intentos fallidos de ingresos no autorizados al sistema.

Se han definido procedimientos periódicos de monitoreo y auditoría para verificar que todos los procesos de gestión de seguridad de la información se llevan adelante adecuadamente.

6.7 CONTROLES DE SEGURIDAD DE LA RED

La infraestructura de la red utilizada por el sistema de la ANC cuenta con todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro donde se destacan los siguientes:

- Se le provee acceso a los usuarios solo a los servicios que les fueron autorizados;
- Se controla, filtra y cifra el acceso desde los clientes hasta los servidores;
- Todo acceso está restringido por defecto y solo se accede con permiso específicamente configurado;
- Los componentes más críticos están totalmente desconectados de Internet;
- Para proteger la red interna de accesos desde redes externas se utiliza un firewall, y se utiliza otro firewall para separar los sistemas de PKI de los demás sistemas de la ANC.

6.8 SELLADOS DE TIEMPO

Todos los sistemas que constituyen la infraestructura de clave pública de la ANC guardan registros de tiempo de todas las actividades. Estos sistemas estarán sincronizados en fecha y hora utilizando como fuente el servidor de la CA.

7 PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 PERFIL DE CERTIFICADO

Los perfiles de los certificados dependen del tipo de certificado y se encuentran especificados en la Política de Certificación correspondiente definida y aprobada por la UCE.

7.2 PERFIL DE CRL

7.2.1 Número de versión

La infraestructura del ANC utiliza CRLs X.509 versión 2 (v2).

7.2.2 CRL y extensiones

Las CRLs emitidas por la PKI de ANC serán conformes con la norma RFC 3280 (Internet X.509 Public Key Infrastructure - Certificate and CRL Profile).

7.3 PERFIL DE OCSP

Los mensajes OCSP se codifican en ASN.1.

7.3.1 Número de versión

El servicio OCSP será conforme con la norma RFC 2560 (X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP).

7.3.2 Extensiones OCSP

No se agregan extensiones.

8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Acorde a las atribuciones delegadas por el gobierno de la República Oriental del Uruguay, la UCE realizará auditorías de cumplimiento con las normativas vigentes y de la adecuación del funcionamiento y operativa con las estipulaciones incluidas en esta CPS.

Las circunstancias y frecuencia de estas auditorías serán definidas por la UCE y podrán consultarse en su página.

Sin perjuicio de lo anterior, personal de la ANC realizará auditorías internas bajo su propio criterio, ya sea para asegurar el cumplimiento o a causa de una sospecha de incumplimiento de alguna medida de seguridad por parte de alguno de sus operadores.

8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Los auditores externos serán auditores acreditados por la UCE de acuerdo a la normativa vigente con los siguientes requerimientos:

- Sociedad comercial con presencia en plaza, inscripta en el Registro Público de Comercio;
- Acreditación de diez años de experiencia en auditoría de sistemas en el área financiera.

Todo equipo o persona designada para realizar una auditoría interna sobre el sistema de PKI deberá cumplir los siguientes requerimientos:

- Adecuada capacitación y experiencia en procesos de auditoría;
- Independencia a nivel organizativo de la CA de ANC.

8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Al margen de la función de auditoría, el auditor externo y la ANC no deberán tener una relación que pudiera derivar en un conflicto de intereses. En el caso de los auditores internos, éstos no podrán tener relación funcional con el área objeto de la auditoría.

8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría determinará la adecuación de los servicios de PKI con los estándares ISO 27001 y Webtrust para Autoridades de Certificación.

8.5 ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

Toda deficiencia significativa detectada por un auditor será objeto de un plan de remediación. El responsable de la CA diseñará dicho plan y realizará el seguimiento de su ejecución.

8.6 COMUNICACIÓN DE RESULTADOS

Los resultados de todas las auditorías realizadas son comunicados al responsable de la CA y a todos los involucrados en la corrección de los aspectos detectados. En aquellos casos donde los hallazgos lo justifiquen, las mismas serán además comunicadas a la Presidencia de la ANC y/o a la UCE.

9 OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 TARIFAS

9.1.1 Tarifas de emisión de certificado o renovación

La ANC cobra únicamente por la emisión y renovación de los certificados digitales que emite. El titular no adquiere ninguna otra deuda por solicitud, acceso, revocación o uso de ningún tipo.

Las tarifas asociadas a cada tipo de certificado podrán variar acorde a las definiciones comerciales de la ANC y no estarán publicadas en esta CPS.

9.1.2 Tarifas de acceso a los certificados

No aplica.

9.1.3 Tarifas de acceso a la información de estado o revocación

No aplica.

9.1.4 Tarifas de otros servicios tales como información de políticas

No aplica.

9.1.5 Política de reembolso

El solicitante tendrá hasta 30 días a partir de la fecha de emisión para solicitar cualquier reclamo. Pasado ese tiempo, se entenderá total aceptación al pago y a la información contenida en el certificado.

En el caso de haberse producido una falla en la emisión y previo a los 30 días, el titular podrá solicitar un reembolso de la totalidad del importe abonado o la reemisión de su certificado sin costo alguno.

Pasados los 30 días no existirán reembolsos ni devoluciones de ningún tipo.

9.2 RESPONSABILIDADES ECONÓMICAS

La ANC se hará cargo de la responsabilidad económica de su PKI por incumplimiento de toda garantía expresa comprometida según los términos de esta CPS y/o CP aplicable, limitándose a los daños directos hasta un monto máximo del costo del certificado en el momento de la compra. En la contratación quedan claros los límites en cuanto al posible uso del Certificado y las transacciones válidas que pueden realizarse empleándolo; notificándose expresamente la limitación cuantitativa de responsabilidad de la que da cuenta la presente cláusula.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

9.3.1 Ámbito de la información confidencial

Toda información que no sea declarada expresamente como pública en esta CPS será el carácter de confidencial.

Se declara expresamente como información confidencial:

• Confidencialidad de la clave privada de la Autoridad de Certificación:

La Autoridad de Certificación garantiza la confidencialidad frente a terceros de su clave privada, la cual será generada y custodiada conforme a lo especificado en esta CPS.

• Confidencialidad de la clave privada de entidades finales:

Para garantizar la confidencialidad de las claves privadas de entidades finales, la Autoridad de Registro de la ANC proporcionará los medios para que la generación de dichas claves solo se realice de modo seguro por el titular o en su presencia.

La Autoridad de Registro y la Autoridad de Certificación no tendrán la posibilidad de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir estas claves.

• Confidencialidad en la prestación de servicios de certificación:

La ANC publicará exclusivamente aquellos datos imprescindibles para la validación de los certificados digitales que emite.

• Protección de datos:

Existe un repositorio de datos personales de los solicitantes con la finalidad de servir a los usos previstos en esta CPS o cualquier otro relacionado con los servicios de PKI.

La ANC no podrá compartir o divulgar estos datos a ninguna otra organización sin el previo consentimiento del titular de la información.

• Registros de auditoría:

Los resultados de auditorías tanto internas como externas son de carácter confidencial.

• Cualquier otra información:

Toda información, clasificada o no como confidencial, a excepción de la expresamente declarada como pública en esta CPS, será de carácter confidencial.

9.3.2 Información no confidencial

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

• La contenida en la presente Declaración de Prácticas de Certificación y las Políticas de Certificación;

• La información sobre el estado de los certificados;

• Toda otra información marcada por la ANC como "Pública".

9.3.3 Responsabilidad de protección de la información confidencial

Los funcionarios de la ANC que participen en cualquier tarea propia o derivada de la PKI están obligados al deber de secreto profesional y, por lo tanto, sujetos a la normativa reguladora que les es aplicable.

9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

9.4.1 Política de protección de datos de carácter personal

Existe un repositorio de datos personales de los solicitantes con la finalidad de servir a los usos previstos en esta CPS o cualquier otro relacionado con los servicios de PKI.

Se permitirá al interesado el ejercicio de los derechos de oposición, acceso, rectificación y cancelación de sus datos de carácter personal en los términos y plazos legales.

9.4.2 Información tratada como privada

Toda información personal no incluida en el certificado o en el proceso de validación del mismo es considerada privada.

9.4.3 Información no calificada como privada

Es considerada no confidencial la siguiente información:

- Los certificados;
- Los usos y límites expresados en el certificado;
- La fecha de emisión del certificado y la fecha de caducidad;
- El número de serie del certificado;
- Los diferentes estados o situaciones del certificado y la fecha de cada uno de ellos.

9.4.4 Responsabilidad de la protección de los datos de carácter personal

Los funcionarios de la ANC que participen en cualquier tarea propia o derivada de la PKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable.

9.4.5 Comunicación y consentimiento para usar datos de carácter personal

El proceso de solicitud de un certificado digital será consentimiento del uso de la información de carácter personal para dicho fin.

9.4.6 Revelación en el marco de un proceso judicial

Los datos de carácter personal solo podrán ser comunicados a terceros, sin consentimiento del afectado, en el marco de un probado proceso judicial.

9.4.7 Otras circunstancias de publicación de información

La ANC podrá enviar la información de la clave pública de un certificado solo con expreso consentimiento del titular y solo a pedido del mismo, para simplificar el procedimiento de uso ante algún otro organismo.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

La ANC es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS.

Esta CPS, así como cualquiera de sus versiones anteriores, son propiedad de la ANC. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos sin la autorización expresa por su parte.

9.6 OBLIGACIONES

9.6.1 Obligaciones de la CA

Es la obligación fundamental de la CA el garantizar la validez y la correspondencia entre los datos contenidos en los certificados que emite, durante todo el período de validez de los mismos.

Por lo tanto, debe estar siempre disponible para atender solicitudes de revocación de certificados, según se detalla en esta CPS.

Otras obligaciones particulares se detallan a continuación:

- Realizar sus operaciones en conformidad con la normativa de la UCE;
- Publicar esta CPS y comunicar los cambios;
- Emitir certificados conformes a la información conocida en el momento de su emisión, y libres de errores de entrada de datos;
- Revocar los certificados en los términos expresados en esta CPS y publicar los certificados revocados en la CRL;
- Publicar el certificado correspondiente a las Autoridades de Certificación de la ANC;
- Proteger la clave privada de la Autoridad de Certificación de la ANC;
- Conservar registrada toda la información y documentación relativa a los certificados que se emiten;
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte;
- No almacenar en ningún caso los datos de creación de firma, clave privada ni claves (PIN ni PUK) de los titulares de certificados;
- Colaborar con los procesos de auditoría;
- Operar de acuerdo con la legislación aplicable.

9.6.2 Obligaciones de la RA

La RA está obligada a verificar, contra presentación de documentación, la identidad del solicitante y toda la información a incluir en un certificado.

La RA se compromete a no hacer público ninguno de los datos aportados por el solicitante en el momento de emisión del certificado.

Otras obligaciones particulares se detallan a continuación:

- Realizar sus operaciones en conformidad con esta CPS;
- Comprobar exhaustivamente la identidad de las personas, así como toda la información incluida o incorporada por referencia en el certificado;
- Informar a entidades finales de las responsabilidades y cuidados que debe tener para su correcto uso;
- Tramitar las peticiones de revocación con celeridad;
- Aprobar la emisión de los certificados luego de asegurar su veracidad;
- No hacer público ninguno de los datos aportados por el solicitante en los términos definidos por esta CPS.

9.6.3 Obligaciones de los titulares de los certificados

Se entiende por titular de un certificado a la persona que tiene acceso o posee la clave privada correspondiente al certificado y es su obligación mantener bajo su custodia dicha clave.

Otras obligaciones particulares se detallan a continuación:

- Suministrar a las Autoridades de Registro información correcta y completa y presentar documentación legítima en el momento de solicitud de un certificado;
- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta CPS, que le sean de aplicación, así como la Política de Certificación que le es aplicable;
- Mantener bajo su custodia y no revelar ni facilitar de manera alguna el acceso a su clave privada para evitar su pérdida, revelación, alteración o uso no autorizado;
- Cumplir y aceptar las restricciones de uso que pudiera haber impuestas a sus claves y certificados en la órbita de PKI Uruguay;
- Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada, entre otras causas, por pérdida, robo, compromiso potencial, conocimiento por terceros de la clave personal de acceso y detección de inexactitudes en la información;
- Asegurarse de que toda la información contenida en su certificado es correcta; de lo contrario, notificarlo inmediatamente.

9.6.4 Obligaciones de los terceros aceptantes

Es tercero aceptante de un certificado toda persona u organismo que, directamente o a través de algún sistema, solicita a terceros la presentación de un certificado, e interpreta su contenido.

Las obligaciones particulares se detallan a continuación:

- Limitar el uso de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados, en esta CPS y en las Políticas de Certificación que le son aplicables;
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas;
- Asumir su responsabilidad en la comprobación de la validez, revocación y estado de los certificados en que confía;
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones;
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

9.6.5 Obligaciones de la UCE

De acuerdo con lo establecido en el artículo 14 de la Ley Nº 18.600, de la Unidad de Certificación Electrónica tendrá los siguientes cometidos y funciones:

1) De acreditación:
- Recibir, tramitar y resolver las solicitudes de acreditación de los prestadores de servicios de certificación;
- 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 la Ley, una vez otorgada la acreditación;
- Suspender o revocar la inscripción de los prestadores de servicios de certificación acreditados;
- 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.

2) De control:
- 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;
- 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;
- Determinar las medidas que estime necesarias para proteger la confidencialidad de los titulares de certificados reconocidos;
- 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.

3) De instrucción:
- 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.

4) De regulación:
- 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;
- 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.

5) De sanción:
- 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.

9.7 LIMITACIONES DE GARANTÍAS

La Administración Nacional de Correos cumple con los requerimientos expresados por artículo 11 del Decreto Nº 436/2011 cumpliendo con los montos establecidos por la UCE.

En la contratación quedan claros los límites en cuanto al posible uso del Certificado y las transacciones válidas que pueden realizarse empleándolo; notificándose expresamente la limitación cuantitativa de responsabilidad de la que da cuenta la presente cláusula.

9.8 LIMITACIONES DE RESPONSABILIDAD

El límite máximo de responsabilidad propuesto en esta CPS será el mismo, independientemente de la cantidad de firmas digitales, transacciones, o reclamaciones relativas al certificado en cuestión. Por otra parte, en la circunstancia de que se sobrepase ese tope, el tope disponible será distribuido de la siguiente forma: primero, a las reclamaciones, según el orden en que fueron presentadas, para alcanzar la solución final del diferendo, a menos que un tribunal competente disponga en contrario.

A excepción de lo establecido por las disposiciones de la presente CPS, la ANC no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

9.9 INDEMNIZACIONES

En ningún caso, la CA estará obligada a pagar más que los montos establecidos, independientemente del método de distribución entre los reclamantes que se aplique al monto total de la indemnización. En la contratación quedan claros los límites en cuanto al posible uso del Certificado y las transacciones válidas que pueden realizarse empleándolo; notificándose expresamente la limitación cuantitativa de responsabilidad de la que da cuenta la presente cláusula.

9.10 PERIODO DE VALIDEZ

9.10.1 Plazo

Esta CPS entra en vigor desde el momento de su publicación en el repositorio de ANC.

Esta CPS se mantendrá en vigor mientras no se derogue expresamente por la emisión de una nueva versión o expire el certificado de la CA a la cual ésta aplica.

9.10.2 Sustitución y derogación de la CPS

Esta CPS será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la CPS quede derogada, se retirará del repositorio público ANC.

9.10.3 Efectos de la finalización

Las obligaciones y restricciones que establece esta CPS en referencia a auditorías, información confidencial, obligaciones y responsabilidades u otras definiciones nacidas bajo su vigencia, vencerán tras su derogación a excepción de los derechos de propiedad intelectual.

En caso de sustitución por una nueva versión, las obligaciones y restricciones que establece esta CPS seguirán vigentes siempre y cuando no se modifiquen en la nueva versión.

9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Las entidades finales podrán comunicarse con la ANC por todas las vías disponibles y publicadas en esta CPS.

La ANC podrá comunicarse tanto a través del correo electrónico expresado como contacto, teléfono de contacto o por correo postal a la dirección registrada.

9.12 CAMBIOS EN LAS ESPECIFICACIONES

9.12.1 Procedimiento para los cambios

La autoridad con atribuciones para realizar cambios sobre esta CPS es la Unidad de Servicios Electrónicos de la ANC. La autoridad con atribuciones para aprobar los cambios es la UCE, de acuerdo a la normativa vigente.

9.12.2 Periodo y procedimiento de notificación

El mecanismo de notificación será la publicación de la nueva versión en el repositorio de la ANC.

9.12.3 Circunstancias en las que el OID debe ser cambiado

La asignación y manejo de los OID es realizado por la UCE de acuerdo a la normativa aplicable.

9.13 RECLAMACIONES Y DISPUTAS

En la eventualidad de cualquier disputa que implique a los servicios o prestaciones que incluye la presente CPS (u otra divulgación de las políticas comerciales de la CA), la parte ofendida notificará primero a la CA y luego a todas las partes interesadas con relación a la disputa. La ANC asignará al personal adecuado para resolver el litigio.

9.14 NORMATIVA APLICABLE

La ley aplicable a este documento será la vigente sobre esta materia en el territorio de la República Oriental del Uruguay, así como los acuerdos internacionales que suscriba el país sobre la misma temática.

9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE

La CA de ANC cumple con toda la normativa vigente como prestador acreditado de acuerdo a la normativa aplicable.

9.16 ESTIPULACIONES DIVERSAS

9.16.1 Cláusula de aceptación completa

Todas las entidades finales y terceros aceptantes asumen la aceptación en su totalidad del contenido de la última versión de esta CPS y la Política de Certificación que le sea aplicable.

9.16.2 Delegación

No estipulado.

9.16.3 Divisibilidad

En el caso de que una o más estipulaciones de esta CPS sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderán por no puestas, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la CPS careciera ésta de toda eficacia jurídica.

9.16.4 Ejecución

Cada caso será tratado por las áreas competentes de la ANC en forma independiente.

9.16.5 Fuerza Mayor

Las áreas competentes de la ANC analizarán particularmente los casos de fuerza mayor que pudieren presentarse, no siendo tratados en esta CPS.

9.17 OTRAS ESTIPULACIONES

No se contemplan.

10 CONTROL DE CAMBIOS

Versión	Cambio	Fecha
1.0	-Versión inicial.	Marzo 2013
1.1	-Cambios en los puntos 3.2.1 y 4.1.2, de acuerdo al cambio en la política de persona física sobre "se debe generar la clave en presencia del PSCA". -Cambios en el punto 5.2.1 por roles que se adecúan a la nueva infraestructura. -Cambios en el punto 9.7, de acuerdo a los montos establecidos por la UCE.	Agosto 2013
1.2	-Cambios en los puntos 2.1 y 4.10.1 para agregar opcionalmente una segunda ubicación de la CRL.	Abril 2015
1.3	-Se quita la modificación anterior para agregar una segunda CRL opcional.	Julio 2017
1.4	-Cambios en los puntos 1.2, 3.3.1 y 4.9.3 con ajustes en los mecanismos de revocación acorde a los cambios en nuevas políticas de UCE.	Abril 2019