Prácticas de Certificación de la Autoridad Certificadora

Historial de Revisiones

Fecha	Descripción	Autor
16/11/2012	Creación del documento	Grupo de SI

Índice de contenido

1 Introducción

1.1 Descripción general

El presente documento describe las Prácticas de Certificación del Prestador de Servicios de Certificación Acreditado Autoridad Certificadora del Ministerio del Interior.

Todos los Prestadores de Servicio de Certificación Acreditados ante la Unidad de Certificación Electrónica (UCE) para la emisión de certificados de persona física, deberán implementar la política descripta en el documento Política de Certificación de persona física elaborado y mantenido por la UCE.

El presente documento se encuentra disponible en formato electrónico en las siguientes URL's:

- http://ca.minterior.gub.uy/politicas/cps-minterior.pdf,
- http://www.uce.gub.uy/politicas/cps-minterior.pdf

o podrá ser solicitado a la Autoridad Certificadora del Ministerio del Interior.

La confección del presente documento se realizó siguiendo la propuesta de estándar para la documentación de políticas y prácticas de certificación del grupo de trabajo IETF PKIX. Dicha propuesta se cataloga como la RFC 3647 [3] en su última versión.

1.2 Identificación

Este documento se titula Prácticas de Certificación de la Autoridad Certificadora.

La fecha de entrada en vigencia de este documento es el 29 de setiembre de 2014 y permanece vigente hasta la liberación de una nueva versión que será notificada a los interesados.

Cualquier cambio realizado a las Prácticas descriptas en este documento deberá ser aprobado por la UCE.

La Autoridad Certificadora del Ministerio del Interior notificará de los cambios que se realicen en este documento mediante la publicación en el sitio web de la institución y cualquier otro medio que entienda necesario.

El oid del presente documento es: 2.16.858.10000157.66565.3.

1.3 Comunidad y ámbito de aplicación

La Ley 18600 de Noviembre de 2009 de Documento Electrónico y Firma Electrónica define la Infraestructura Nacional de Certificación Electrónica como el conjunto de equipos y programas informáticos, dispositivos criptográficos, políticas, normas y procedimientos, dispuestos para la generación, almacenamiento y publicación de los certificados electrónicos reconocidos, así como también para la publicación de información y consulta del estado de vigencia y validez de dichos certificados.

En dicha ley se definen, entre otros, los prestadores de Servicios de Certificación Acreditados, la Autoridad de Certificación Nacional y la Unidad de Certificación Electrónica.

1.3.1 Ente Regulador

El rol de Ente Regulador es desempeñado por la UCE y sus funciones están estipuladas en la Política de Certificación de la Autoridad Certificadora Raíz Nacional (ACRN).

1.3.2 Autoridades Certificadoras

En la Public Key Infrastructure (PKI) Uruguay se visualizan varias Autoridades de Certificación entre la cuales se puede distinguir la ACRN (root-CA) y las Autoridades Certificadoras de los Prestadores Acreditados (ACPA).
Su descripción y roles se pueden encontrar en la Política de Certificación de persona física de la UCE.

1.3.3 Autoridades de Registro

Las Autoridades de Registro brindan servicios a los usuarios finales de los distintos ACPA, sus funciones se encuentran descriptas en la Política de Certificación de persona física de la PKI Uruguay.

1.3.4 Suscriptores

Se considera como suscriptores a toda persona física que voluntariamente confíe y utilice los certificados emitidos por el Prestador de Servicios de Certificación. Sus funciones se describen en la Política de Certificación de persona física.

1.3.5 Terceras partes de Confianza

Por terceras partes de confianza se entienden todas las personas o entidades que confían en los certificados emitidos por el Prestador de Servicios Certificador Acreditado (PSCA).

Sus funciones se describen en la Política de Certificación de persona física.

1.3.6 Otros participantes

No es aplicable en este contexto.

1.4 Aplicabilidad

1.4.1 Usos Permitidos de los Certificados

Los usos habilitados para los certificados de persona física emitidos siguiendo las prácticas descriptas en el presente documento se encuentran en la Política de Certificación de persona física de la PKI Uruguay.

1.4.2 Restricciones en el Uso de los Certificados

Los certificados emitidos por la ACPA Autoridad Certificadora del Ministerio del Interior se rigen por las restricciones descriptas en el documento Política de Certificación de persona física.

1.5 Datos de contacto

Para contactar la ACPA Autoridad Certificadora del Ministerio del Interior están habilitados los siguientes medios de comunicación:

- Sitio Web: http://ca.minterior.gub.uy
- Teléfono: 1528888
- Fax: 1528888
- Correo Electrónico: ca.soporte@minterior.gub.uy

- Dirección: Julio Herrera y Obes 1466 Piso 3

1.6 Administración de la Práctica de Certificación

La Administración de la presente Declaración de Prácticas de Certificación es responsabilidad del Ministerio del Interior.

Por consultas o sugerencias, el Ministerio del Interior designa al siguiente contacto:

Nombre: Ministerio del Interior

Dirección de correo: ca.contacto@minterior.gub.uy

Teléfono: 1528888

1.7 Relación entre la Declaración Prácticas de Certificación y otros documentos

Este documento contiene la Declaración de Prácticas de Certificación de Autoridad Certificadora del Ministerio del Interior.

Estas prácticas de certificación describen como se realiza la emisión y gestión de certificados electrónicos, con soporte de claves públicas que pueden utilizarse en diferentes servicios.

Para la definición e implementación de dichas prácticas se siguen las reglas definidas por la Política de Certificación de persona física de la PKI Uruguay.

La presente Declaración de Prácticas de Certificación cumplimenta lo dispuesto por la ley 18600.

Esta documentación se relaciona con la Política de Certificación de persona física así como con documentación auxiliar, documentación de seguridad, documentación de operación y documentación de archivo, entre otras.

1.8 Procedimiento de Aprobación

Las presentes prácticas son elaboradas por parte del Ministerio del Interior en cumplimiento de las normativas vigentes para ser ACPA y el mismo asegura la implementación de procedimientos que aseguren el correcto mantenimiento de la Declaración de Políticas de Certificación.

Adicionalmente y previo a la publicación de la presente declaración la misma fue aprobada por la UCE para garantizar que los procedimientos descriptos siguen las políticas definidas en la PKI Uruguay.

De la misma forma el Ministerio del Interior se compromete a la aplicación de las prácticas definidas, teniendo como ente de contralor la UCE.

1.9 Definiciones y abreviaturas

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

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

Autoridad Certificadora del Prestador Acreditado (ACPA): suscriptor de los certificados

emitidos por la ACRN que, durante su operativa, emite certificados a usuarios finales bajo las políticas de certificación que le fueron asignadas.

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

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

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

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

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

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

2 Aspectos Generales

2.1 Obligaciones y derechos

2.1.1 Obligaciones de la Unidad Reguladora

Obligaciones de la UCE

La Ley 18600 crea la UCE como el ente regulador de la PKI Uruguay. En las Políticas de Certificación de la ACRN se especifican las obligaciones que la misma tiene respecto a toda la Infraestructura Nacional de Certificación.

2.1.2 Obligaciones del certificador

Obligaciones de la ACRN

Las obligaciones de la ACRN como entidad certificadora raíz se encuentran descriptas en la Política de Certificación de la ACRN.

Obligaciones de la Autoridad de Registro de la ACRN

Las obligaciones de la autoridad de registro de la ACRN se encuentran descriptas en la Política de Certificación de la ACRN.

Obligaciones de los Prestadores de Servicios de Certificación Acreditados

Las obligaciones de los PSCA se encuentran descriptas en la política de certificación de la ACRN.

Obligaciones de las ACPA

Las obligaciones de cada Autoridad de Certificación de un Prestador Acreditado se encuentran descriptas en la Política de Certificación de la ACRN.

Obligaciones de las Autoridades de Registro de los Prestadores Acreditados

Las obligaciones de las Autoridades de Registro de las ACPA son asumidas por el prestador de Servicios o por las instituciones que hayan sido mandatadas a estas instancias, dichas obligaciones se encuentran descriptas en la Política de Certificación de la ACRN.

2.1.3 Obligaciones de los Terceros aceptantes

Las obligaciones de los Terceros Aceptantes se encuentran descriptas en la Política de Certificación de persona física.

2.1.4 Obligaciones del servicio de repositorio de la PKI Uruguay

Las obligaciones se encuentran descriptas en la Política de Certificación de la ACRN.

2.2 Responsabilidades

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

2.3 Interpretación y ejecución de las Normas

Estipulado en la Política de Certificación de persona física.

2.4 Tarifas

El Ministerio del Interior se reserva el derecho de aplicar tarifas para la emisión y renovación de certificados.

2.5 Publicación y Repositorios de Certificados y listas de certificados revocados (CRL)

2.5.1 Publicación de información del certificador

Se establece que la Autoridad Certificadora del Ministerio del Interior cuenta con el siguiente sitio web como repositorio público de información:

- ca.minterior.gub.uy

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 del Ministerio del Interior, éste dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

La información mínima que el Ministerio del Interior se compromete a publicar y que se encuentra estipulada en la “Política de Certificación de persona física” en el punto 2.5.1 es la siguiente:

- Política de Certificación de persona física de la PKI Uruguay.
- El presente documento con las Prácticas de Certificación.
- Perfiles de los Certificados Emitidos.
- Lista de Certificados Revocados de la Autoridad Certificadora del Ministerio del Interior con una periodicidad diaria en la *url* definida como *distribution point* en los certificados.
- Auditorías Realizadas.
- Información de Identificación y contacto del Ministerio del Interior.

2.5.2 Frecuencia de publicación

El Ministerio del Interior cumple con la frecuencia de publicación establecida en la Política de Certificación de persona física de la PKI Uruguay.

2.5.3 Controles de acceso a la información

El Ministerio del Interior brinda acceso irrestricto a toda la información publicada en el repositorio público y establece los controles necesarios para restringir la escritura y/o modificación de la información publicada.

2.5.4 Repositorios de certificados y listas de revocación

El Ministerio del Interior se compromete a mantener los repositorios públicos de información disponibles las 24hs los 7 días de la semana y en caso de tener problemas solucionarlos en un tiempo no mayor a las 48hs siempre y cuando el problema se encuentre en el ámbito de control del Ministerio del Interior.

2.6 Auditoría

El Ministerio del Interior se compromete a realizar Auditorías periódicas así como a permitir ser auditado por la UCE cuando la misma considere necesario.

El resultado de las auditorías será publicado en el repositorio público de información.

2.7 Confidencialidad

El Ministerio del Interior cumple con lo estipulado en la Política de Certificación de persona física.

2.8 Propiedad intelectual

El Ministerio del Interior mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la documentación y a publicaciones pertenecientes a ella.

Este documento podrá reproducirse o distribuirse atribuyendo su autoría al Ministerio del Interior en forma precisa, completa y sin modificaciones.

3 Identificación y Autenticación

3.1 Registro inicial

En el contexto de la presente declaración de Practicas de Certificación de la Autoridad Certificadora del Ministerio del Interior, la Identificación y Autenticación se refiere al procedimiento mediante el cual la persona física, hace la solicitud a la autoridad de certificación de un certificado, en la autoridad de registro se valida la documentación presentada y se habilita la generación del certificado.

Las personas físicas que deseen solicitar un certificado emitido por el Ministerio del Interior deben realizar la solicitud de forma presencial.

Se debe presentar ante la Autoridad de Registro del Ministerio del Interior la documentación solicitada. Las autoridades de registro del Ministerio del Interior son la Dirección Nacional de Identificación Civil (DNIC) para el público en general, y el Departamento de Informática de Secretaría del Ministerio para emisiones extraordinarias aprobadas explícitamente. Los siguientes requerimientos aplican a ambas autoridades de registro en forma indistinta.

3.1.1 Nominación

Los certificados emitidos por el Ministerio del Interior son certificados X.509 v3, se utilizará el campo *DistinguishedName* para identificar a la persona, de acuerdo al formato especificado en el punto 3.1.1.1 de la Política de Certificación de persona física.

3.1.2 Validación inicial de identidad

Las personas que deseen solicitar un certificado de persona física ante el Ministerio del Interior deberán presentar ante la autoridad de registro un documento de identidad vigente, en buenas condiciones y que contenga la foto del solicitante.

3.1.3 Clave Privada

Para la emisión del certificado de persona física, se deberá generar un par de claves asignadas a la persona que está realizando la solicitud.

La generación de dichas claves depende del dispositivo donde se desee realizar.

El Ministerio del Interior prevé el mecanismo de Solicitud Presencial, mediante el cual el solicitante se presenta ante la Autoridad de Registro para hacer la solicitud y en el mismo acto se valida la documentación y se generan las claves en un Dispositivo Seguro de Creación de Firmas (DSCF) (hardware) provisto por la Autoridad de Registro (AR).

3.1.4 Identificación y autenticación para solicitudes de cambio de clave

No aplica en la presente definición de Prácticas.

3.1.5 Identificación y autenticación para solicitudes de revocación

Las personas físicas que cuenten con un certificado emitido por el Ministerio del Interior podrán solicitar la revocación de su certificado.

Para realizar dicha solicitud la persona deberá presentarse ante la Seccional Policial mas cercana

con la documentación que los identifique como el suscriptor del certificado. En caso que la persona no cuente con la documentación que lo avale como suscriptor, o que la Seccional no tenga acceso al sistema del Ministerio, deberá responder telefónicamente un reto de seguridad para autenticar la solicitud.

Además, se encuentra habilitada una vía de auto revocación mediante firma electrónica de una petición a través del sitio web de la AC, ca.minterior.gub.uy.

La revocación y publicación de la nueva CRL se realizará en un plazo inferior a 2 horas.

4 Requerimientos Operativos del Ciclo de Vida de los Certificados

4.1 Solicitud de certificado

De acuerdo a la Política de Certificación de persona física.

4.1.1 Legitimación para solicitar la emisión

La documentación a presentar para la solicitud del certificado de persona física es la cédula de identidad o pasaporte en el caso de extranjeros, ambos vigentes y en buen estado.

4.1.2 Registro de las solicitudes de certificados

El titular debe presentarse en un puesto de registro habilitado para la emisión de certificados, en dicho puesto se validarán los datos, y el operador de registro completará el formulario web de solicitud y generará las claves en un DSCF provisto por la AR. Una vez validada la solicitud continuará el procedimiento de emisión del certificado.

Para el público en general los puestos de registro habilitados son las oficinas de la Dirección Nacional de Identificación Civil (DNIC). Para emisiones excepcionales aprobadas por el Departamento de Informática de Secretaría, se encuentra habilitado éste como puesto de registro y emisión, actuando en ese caso sus funcionarios como oficiales de registro.

4.2 Proceso de requerimiento del certificado

El operador de registro corroborará la información presentada por el solicitante con la provista por DNIC, pudiendo aprobar o denegar la solicitud en el sistema y realizar cambios en los datos en caso de ser necesario.

Una vez confirmados los datos contra los provistos por DNIC, el operador de registro aprueba la solicitud, la cual es enviada automáticamente a la AC para la emisión del certificado.

4.3 Emisión de certificado

La Autoridad Certificadora del Ministerio del Interior procede a la emisión de los certificados correspondientes a las solicitudes aprobadas desde la Autoridad de Registro.

Los Certificados se generan de forma que se vincule el certificado con la información de registro de forma segura e incluyen la clave pública firmada.

Una vez emitido el certificado, el sistema notifica al operador de registro, quien descargará el certificado en el dispositivo criptográfico utilizado para la generación de la solicitud en primer lugar.

4.4 Aceptación de certificado

El operador de la AR muestra el certificado generado al suscriptor para su aceptación.

En el caso de que no se acepte el certificado por parte del suscriptor, por la razón que sea, se procederá a realizar la revocación del mismo por parte del operador de la Autoridad de Registro, en concordancia con el numeral 4.9 del presente documento.

4.5 Uso del Certificado y de Par de Claves

El usuario final debe utilizar la clave privada asociada a su certificado emitido por el ACPA para los usos descriptos en el punto 1.4 de la Política de Certificación de persona física.

4.6 Renovación del certificado

No se realizan renovaciones de certificados.

4.7 Cambio de Clave del Certificado

No se realizan cambios de claves de los certificados.

4.8 Modificación del certificado

No se realizan modificaciones de certificados. Para estos casos el titular deberá solicitar primero una revocación del certificado vigente y posteriormente la solicitud de un nuevo certificado.

4.9 Revocación y suspensión del certificado

No se realizan suspensiones de los certificados.

4.9.1 Causas para la revocación

Las causas de revocación se encuentran descriptas en la Política de Certificación de persona física.

4.9.2 Legitimación para solicitar la revocación

Podrán solicitar la revocación del certificado las personas o entidades especificadas en la Política de Certificación de persona física.

4.9.3 Procedimientos de solicitud de revocación

La solicitud de revocación de un certificado deberá realizarse de forma presencial por parte del titular del mismo en la Seccional Policial más cercana en la cual se requerirá los datos del titular. En caso que la Seccional no se encuentre conectada al sistema central del Ministerio del Interior el suscriptor deberá contestar una serie de preguntas de seguridad para validar su identidad.

La AR que realiza la revocación deja constancia de las causales de revocación, registrando:

- Fecha/Hora
- Solicitante
- Mecanismo de comprobación de la solicitud de revocación
- Motivo
- Operador actuante

En caso que el suscriptor ingrese su petición de auto-revocación a través del sitio web del Ministerio destinado a tal fin, el operador de la AC es quien realiza la validación de la solicitud, la revocación y la generación de los registros anteriormente mencionados.

4.9.4 Plazo temporal de solicitud de revocación

La revocación se llevará en un plazo menor a 2 horas una vez comprobada la autenticidad de la

solicitud.

4.9.5 Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación se procesa en el mínimo plazo posible. Nunca mayor a 24 horas.

4.10 Servicios de estado del certificado

El Ministerio del Interior se compromete a publicar la CRL en su repositorio. El Ministerio del Interior no se responsabiliza por cualquier tipo de incidente que derive de la falta de verificación de la CRL de la Autoridad Certificadora del Ministerio del Interior o la de la ACRN por parte de terceros aceptantes.

4.11 Fin de la suscripción

La finalización de la suscripción refiere a las situaciones en las que el certificado alcance su fecha de expiración.

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

4.12 Archivado y recuperación de clave

No se prevé el archivado y recuperación de claves para los certificados de persona física de la Autoridad Certificadora del Ministerio del Interior.

5 Controles de Seguridad Física, de Procedimiento y de Personal

5.1 Controles de seguridad física

La AC 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:

1. delimitación de las áreas seguras e inseguras en las instalaciones donde se procesan o almacenan claves criptográficas y certificados;
2. medidas para impedir el acceso no autorizado a las instalaciones a través de puertas, ventanas y muros;
3. 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);
4. medidas restrictivas para el acceso a las áreas seguras dentro de la organización (ingreso del mínimo personal requerido);
5. medidas de detección del acceso en áreas vacantes (sensores de movimientos, alarmas, cámaras de video);
6. medidas para el control de la temperatura del equipamiento en funcionamiento;
7. medidas de protección contra incendios (detectores de humo, extintores de polvo);
8. medidas de protección contra inundaciones (de acuerdo a la evaluación de riesgos de inundación);
9. 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:

1. Inventario actualizado de los sistemas y medios de almacenamiento de la organización;
2. procedimientos para el ingreso y egreso de sistemas y medios a la organización, que requieren la aprobación explícita de los niveles gerenciales;
3. procedimientos para la destrucción física de medios de almacenamiento;
4. política de escritorios limpios, retirando de las áreas de trabajo aquella información que no esté siendo utilizada.

5.2 Controles Procedimentales

Los procesos que permiten el funcionamiento de la AC 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 AC:

- 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 AC 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 AC 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 AC son mantenidos en su directorio por tiempo indefinido, incluso luego de su expiración y/o revocación.

5.6 Cambio de Claves

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

5.7 Continuidad de Operaciones

La AC 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 AC están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control del Ministerio del Interior, éste dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

5.8 Terminación de las Operaciones

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

6 Controles de Seguridad Técnica

6.1 Instalación del Equipamiento Informático

El equipamiento dedicado a la gestión de los certificados fue instalado ante la presencia de Auditores autorizados por la UCE, certificando su correcta instalación.

6.2 Generación e instalación del par de claves

6.2.1 Generación del par de claves

Generación del Par de Claves de la AC

Los requisitos para la generación del par de claves para una AC se encuentran en las Políticas de Certificación de la ACRN en el punto 6.2.2. El par de Claves de la Autoridad Certificadora del Ministerio del Interior fue generada cumpliendo con dicha política.

Generación del Par de Claves para persona física

Tanto la DNIC como el Departamento de Informática de Secretaría del Ministerio, como Autoridades de Registro, generan las claves en un DSCF provisto por el Ministerio del Interior. El suscriptor en este momento elige un PIN para protegerlas.

6.2.2 Entrega de la clave privada al titular

La clave privada nunca abandona el DSCF donde se genera y se le entrega al solicitante protegida por este.

6.2.3 Entrega de la clave pública al emisor del certificado

La generación del par de claves se realiza en el DSCF, tanto la DNIC como el Departamento de Informática de Secretaría del Ministerio en su rol de Autoridades de Registro obtienen la clave pública directamente del DSCF.

6.2.4 Longitud de las claves

Las claves los certificados de persona física son de 2048 bits.

6.2.5 Fines de uso de las claves

Los pares de claves correspondientes a los certificados de persona física pueden ser utilizados para los usos indicados en el punto 1.4 de la Política de Certificación de persona física.

6.3 Protección de la clave privada

Las claves privadas de los certificados de persona física son generadas en un DSCF provisto por el Ministerio del Interior.

En ningún caso se realizan copias o queda residuo alguno de las claves en los equipos de la AR o

en los sistemas de la AC.

Es responsabilidad del solicitante la correcta gestión y protección de su clave privada.

6.4 Otros aspectos de la gestión del par de claves

No Aplica.

6.5 Datos de activación

Para hacer uso de su clave privada, los suscriptores deben activarla previamente mediante el ingreso de un PIN, elegido al momento de la generación.

6.6 Controles de seguridad informática

El acceso a los sistemas de la Autoridad Certificadora del Ministerio del Interior esta restringido a personal autorizado mediante controles de acceso a usuarios a los sistemas operativos y a las aplicaciones de la AC.

Se definen como parte de sus políticas de operación, roles y responsabilidades, identificación y autenticación de usuarios, segregación de tareas y controles múltiple persona para tareas criticas.

Se utiliza doble factor para la autenticación de los usuarios en los subsistemas de la AC.

Todos los subsistemas de la AC son fiables de acuerdo a la especificación técnica CWA 14167-1.

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

El Ministerio del Interior cuenta con un inventario actualizado con los sistemas de información y medios de almacenamiento asociados a la operación de la AC.

Por otra parte, el Ministerio cuenta con procesos de actualización y aplicación de parches críticos sobre los sistemas de operación de la AC.

6.8 Seguridad de la red

La red de la AC del Ministerio del Interior cumple con todos los requisitos necesarios para garantizar la correcta seguridad de los sistemas.

La misma cuenta con esquemas de seguridad en profundidad así como segmentación en zonas de confianza.

Únicamente los usuarios con los permisos necesarios pueden acceder a los distintos subsistemas.

Ningún equipo de producción de la AC que contenga datos críticos esta expuesto directamente a Internet.

6.9 Sincronización Horaria

Todos los equipos de la Infraestructura de Certificación del Ministerio del Interior se sincronizan utilizando los equipos previstos a tales fines.

Es responsabilidad de los suscriptores hacer uso de sus certificados en equipos con la fecha y hora correctas.

7 Perfiles de Certificado y CRL

7.1 Perfil de certificado de persona física

Los certificados de persona física emitidos por la Autoridad Certificadora del Ministerio del Interior utilizan el estándar X.509 versión 3 de acuerdo con el perfil establecido en la RFC 5280.

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la AC
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	C = UY O = Ministerio del Interior CN = Autoridad Certificadora del Ministerio del Interior
Validez (Valid From / Valid To)	0 a 2 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	CN = Nombre completo de la persona física C = País del Documento de identificación presentado serialNumber = Código y número de documento (Ver sección 3.1.1)
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 2048 bits
Extensiones	
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Identificador de la clave de la autoridad (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la AC del Ministerio del Interior
Uso de Claves (Key Usage)	DigitalSignature = 1 NonRepudiation/contentCommitment = 1 KeyEncipherment = 1 DataEncipherment = 1 KeyAgreement = 0 KeyCertSign = 0 CRLSign = 0 EncipherOnly = 0 DecipherOnly = 0
Uso de Claves Extendido (Extended Key Usage)	clientAuth
Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.2 URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_persona_fisica.pdf OID: 2.16.858.10000157.66565.3 URI: https://ca.minterior.gub.uy/politicas/cps.pdf
Restricciones Básicas (Basic	CA = FALSE

Constraints)	
Puntos de distribución de las CRL (CRL Distribution Points)	URI = http://ca.minterior.gub.uy/crls/ca.crl URI = URL secundaria de publicación de la CRL

7.2 Perfil de la CRL

Las listas de certificados revocados o listas de revocación emitidas por la Autoridad Certificadora del Ministerio del Interior utilizan el estándar X.509 versión 2 de acuerdo con el perfil establecido en la RFC 5280.

Atributos	**Contenido**
Versión (Version)	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	C = UY O = Ministerio del Interior CN = Autoridad Certificadora del Ministerio del Interior
Día y Hora de Emisión (Efective Date)	Día y hora de la emisión de esta CRL
Próxima Actualización (Next Update)	Día y hora de la próxima actualización planificada de la CRL
Certificados Revocados (Revoked Certificates)	Lista de los certificados revocados. Incluye número de serie (Serial Number), fecha de revocación (Revocation Date) y motivo (Reason Code).
Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la AC
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

8 Administración Documental

8.1 Procedimiento para cambio de especificaciones

El Ministerio del Interior cuenta con procedimientos internos para la administración de los cambios sobre la presente Declaración de Prácticas de Certificación.

En dichos procedimientos se prevé el envío de las modificaciones a la UCE para su aprobación.

8.2 Procedimientos de Publicación y Notificación

El Ministerio del Interior publicará en su repositorio público las modificaciones aprobadas por la UCE en la presente declaración indicando en cada caso, las secciones o textos que se modificaron.

En caso de ser modificaciones importantes, el Ministerio del Interior notificará a todos los suscriptores de sus certificados.

Dichas modificaciones serán publicadas en http://ca.minterior.gub.uy y los usuarios serán notificados vía correo electrónico.

9 Documentos Externos

1. Política de Certificación de persona física de la ACRN (http://www.uce.gub.uy/acrn/cp_acrn.pdf)
2. Declaración de Practicas de certificación de la ACRN (http://www.uce.gub.uy/acrn/cps_acrn.pdf)
3. RFC 3647 – Internet Engineering Task Force (IETF) (http://www.ietf.org/rfc/rfc3647.txt)