

Política de Certificación de Persona Jurídica

Versión 2.0

Unidad de Certificación Electrónica

Infraestructura Nacional de Certificación Electrónica
República Oriental del Uruguay

Índice

1.Introducción.....	4
1.1.Descripción general.....	4
1.1.Identificación de la Política de Certificación	6
1.2.Participantes de la INCE.....	7
1.2.1.Unidad Reguladora.....	7
1.2.2.Autoridad Certificadora.....	7
1.2.3.Autoridad de Registro	8
1.2.4.Suscriptores	9
1.2.5.Terceros Aceptantes.....	9
1.2.6.Otros participantes.....	10
1.3.Uso de los certificados.....	10
1.3.1.Usos Permitidos de los Certificados	10
1.3.2.Restricciones en el Uso de los Certificados.....	10
1.4.Administración de la Política de Certificación	10
1.5.Relación entre la Política de Certificación y otros documentos.....	11
1.6.Procedimiento de Aprobación.....	11
1.7.Definiciones y abreviaturas	11
2.Aspectos Generales de la Política de Certificación	16
2.1.Obligaciones	16
2.1.1.Obligaciones de la Unidad Reguladora	16
2.1.1.1.Obligaciones de la UCE.....	16
2.1.2.Obligaciones del Certificador.....	17
2.1.2.1.Obligaciones de la ACRN	17
2.1.2.2.Obligaciones de los PSCA	17
2.1.3.Obligaciones de las Autoridades de Registro de los Prestadores Acreditados.....	18
2.1.4.Obligaciones de los Suscriptores de Certificados.....	19
2.1.5.Obligaciones de los Terceros Aceptantes.....	21
2.1.6.Obligaciones del servicio de repositorio de la INCE.....	22
2.2.Responsabilidades	24
2.3.Tarifas	24
2.4.Interpretación y aplicación de las normas.....	25
2.4.1.Legislación aplicable.....	25
2.4.2.Forma de interpretación y aplicación	25
2.4.3.Procedimientos de resolución de conflictos	25
2.5.Publicación y Servicios de Estado de Certificados.....	26
2.5.1.Publicación de información del certificador.....	26
2.5.2.Frecuencia de publicación	26

2.5.3. Controles de acceso a la información	27
2.5.4. Repositorios de certificados y listas de revocación	27
2.6. Auditoría	27
2.7. Confidencialidad	28
2.7.1. Publicación de Información sobre los PSCA	28
2.7.2. Publicación de Información sobre los Suscriptores Finales	28
2.7.3. Publicación de Información sobre Revocación de Certificados	28
2.7.4. Divulgación de información a autoridades judiciales	29
2.7.5. Divulgación de información por solicitud del suscriptor	29
2.7.6. Otras circunstancias de divulgación de información	29
2.8. Derechos de propiedad intelectual	29
3. Identificación y Autenticación	30
3.1. Registro inicial	30
3.1.1. Nominación	30
3.1.1.1. Formato del Nombre Distinguido	30
3.1.2. Validación inicial de identidad	32
3.1.2.1. Identidad	32
3.1.2.2. Clave Privada	32
3.1.3. Identificación y autenticación para solicitudes de cambio de clave	33
3.1.4. Identificación y autenticación para solicitudes de desvinculación de referente	33
3.1.5. Identificación y autenticación para solicitudes de vinculación de referente	33
3.1.6. Identificación y autenticación para solicitudes de revocación	34
4. Requerimientos Operativos del Ciclo de Vida de los Certificados	35
4.1. Solicitud de certificado	35
4.1.1. Legitimación para solicitar la emisión	35
4.1.2. Registro de las solicitudes de certificados	36
4.2. Procesamiento del requerimiento de certificado	37
4.3. Emisión de certificado	37
4.4. Aceptación de certificado	38
4.5. Uso del Certificado y del Par de Claves	38
4.6. Renovación del certificado	39
4.7. Cambio de Clave del Certificado	40
4.8. Modificación del certificado	41
4.9. Desvinculación del referente del certificado	41
4.10. Vinculación de un nuevo referente del certificado	41
4.11. Revocación y suspensión del certificado	42
4.11.1. Causas para la revocación	42
4.11.2. Legitimación para solicitar la revocación	43
4.11.3. Procedimiento de revocación	43
4.11.4. Plazo máximo de procesamiento de la solicitud de revocación	44
4.11.5. Comprobación del estado de revocación de un certificado	44

4.12. Servicios de estado del certificado	45
4.13. Fin de la suscripción.....	45
4.14. Archivado y recuperación de clave	46
5. Controles de Seguridad Física, de Procedimiento y de Personal.....	47
5.1. Controles de seguridad física.....	48
5.2. Controles procedimentales.....	49
5.3. Controles de seguridad del personal	50
5.4. Controles para registros de auditoría	51
5.5. Procedimiento para el cambio de certificado de la ACPA.....	52
5.6. Procedimientos para recuperación de desastres	52
5.7. Procedimientos para terminación de las operaciones	53
6. Controles de Seguridad Técnica	54
6.1. Instalación del equipamiento informático de la ACPA	54
6.2. Generación e instalación del par de claves	54
6.2.1. Generación e instalación del par de claves de la ACPA	54
6.2.2. Generación del par de claves para Persona Jurídica	54
6.3. Protección de la clave privada	55
6.3.1. Protección de la clave privada de la ACPA	55
6.3.2. Protección de la clave privada de la Persona Jurídica.....	55
6.4. Otros aspectos de la gestión del par de claves	56
6.5. Datos de activación.....	56
6.6. Controles de seguridad informática	56
6.7. Controles de seguridad sobre el ciclo de vida de los sistemas	57
6.8. Seguridad de la red	57
6.9. Sincronización horaria	57
7. Perfiles de Certificado y CRL.....	58
7.1. Perfil de certificado de Persona Jurídica.....	58
7.2. Perfil de la CRL de las ACPA de PSCA.....	60
8. Administración Documental	61
8.1. Procedimiento para cambio de especificaciones	61
8.2. Procedimientos de Publicación y Notificación	61
Referencias Externas	62

1.Introducción

1.1. Descripción general

Según el inciso 2º, del artículo 21 del Código Civil: "Se consideran personas jurídicas y por consiguiente capaces de derechos y obligaciones civiles, el Estado, el Fisco, el Municipio, la Iglesia y las corporaciones, establecimientos y asociaciones reconocidas por la autoridad pública."

Un Certificado Electrónico Reconocido de Persona Jurídica (CERPJ), en el contexto de la Infraestructura Nacional de Certificación Electrónica (INCE – PKI Uruguay), es un certificado electrónico emitido por un Prestador de Servicios de Certificación Acreditado (PSCA) a una Persona Jurídica previamente identificada. Este certificado le permite al sistema portador realizar firmas electrónicas avanzadas y a un tercero verificar que el emisor de un documento electrónico emanado de un sistema es la persona jurídica titular del mismo.

A nivel conceptual, la Firma Electrónica Avanzada consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a documentos electrónicos. La clave privada siempre se encuentra en posesión del firmante y es la utilizada para realizar firmas. La pública se divulga y es la utilizada para verificar una firma de otro sujeto.

El Certificado de Persona Jurídica establece una asociación directa entre la identidad de la Persona Jurídica y su clave pública, con el respaldo brindado por la INCE. Esta asociación clave pública-persona jurídica es un componente imprescindible para la realización de una Firma Electrónica Avanzada en Uruguay, ya que es la que permite a alguien, que verifica una firma, identificar al firmante.

La raíz de confianza de la INCE - PKI Uruguay es la Autoridad Certificadora Raíz Nacional (ACRN), operada por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Un PSCA es una persona física o jurídica, pública o privada, poseedora de una o varias Autoridades Certificadoras de Prestador Acreditado (ACPA), cada una de ellas con un

Certificado Electrónico Reconocido (CER) emitido por la ACRN, constituyendo el segundo eslabón de la cadena de confianza y emitiendo Certificados Electrónicos Reconocidos a usuarios finales. Los suscriptores finales interactúan con los PSCA a través de sus Autoridades de Registro (RA) para la solicitud de emisión, renovación y revocación de certificados electrónicos reconocidos.

Una Política de Certificación es un conjunto de principios y normas que describen el perfil de un Certificado; sus usos permitidos, los derechos y obligaciones de todos los actores involucrados en su utilización, los procesos mediante los cuales se verifica la identidad del titular del Certificado, se generan las claves, se emite y se revoca el Certificado y las garantías tecnológicas de seguridad que el PSCA aplica en cada caso. En el contexto de la INCE, las Políticas de Certificación son desarrolladas y aprobadas por la UCE.

La presente Política de Certificación de Persona Jurídica rige la actividad de los PSCA que emiten certificados a personas jurídicas. De esta manera se asegura, independientemente del PSCA que haya emitido el certificado particular, la uniformidad de garantías, políticas de uso y aspectos técnicos de los certificados de Persona Jurídica, incluyendo la interoperabilidad natural entre sistemas que hagan uso de los mismos, ya que se trata de un estándar común para todos los PSCA.



La actividad de los PSCA se encuentra regulada por la Unidad de Certificación Electrónica (UCE) y sujeta a sus procedimientos de control. A su vez, cada PSCA presenta a la UCE un documento denominado Declaración de Prácticas de Certificación en el cual declara los procedimientos administrativos y técnicos mediante los cuales satisface lo exigido por la Política de Certificación. La UCE valida este documento previamente a que el Prestador comience la operación de una ACPA.

La confección del presente documento se realizó siguiendo el marco normativo vigente y la propuesta de estándar para la documentación de Políticas y Declaración de Prácticas de Certificación del grupo de trabajo IETF PKIX. Dicha propuesta se denomina RFC 3647 en su última versión [1].

1.1. Identificación de la Política de Certificación

Nombre: Política de Certificación de Persona Jurídica

Versión: 2.0

Fecha de elaboración: 31/10/2012

Fecha de última actualización: 14/11/2024

OID: 2.16.858.10000157.66565.4

Sitio web de publicación: <https://www.gub.uy/unidad-certificacion-electronica/comunicacion/publicaciones/politica-certificacion-persona-juridica>

1.2. Participantes de la INCE

1.2.1. Unidad Reguladora

El rol de Unidad Reguladora es desempeñado por la UCE, según lo dispuesto por la Ley N° 18.600, de 21 de Setiembre de 2009 [2], es un rol de regulación, en el cual debe definir los estándares técnicos y operativos que deberán cumplir los PSCA, así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.

Además de su rol regulador, la UCE desempeña funciones de acreditación de Prestadores de Servicios de Certificación; control y auditoría de su actividad; instrucción estableciendo criterios generales y asesoramiento en buenas prácticas de funcionamiento; y sanción en caso de incumplimiento. Puede encontrarse información detallada en la Política de Certificación de la ACRN [3] y en el artículo 14 de la Ley N° 18.600, de 21 de Setiembre del 2009 [2].

1.2.2. Autoridad Certificadora

Los Prestadores de Servicios de Certificación Acreditados son organismos públicos o privados que pertenecen a la INCE y emiten certificados electrónicos a usuarios finales.

Para la emisión de certificados, los PSCA podrán operar al menos una Autoridad Certificadora. A esta Autoridad se la denomina Autoridad Certificadora del Prestador Acreditado (ACPA) y consiste en el conjunto de sistemas, personas, políticas y procedimientos relativos a la gestión de certificados electrónicos.

Cuando el PSCA registra a una ACPA, la ACRN le emite un certificado según lo estipulado en la Política de Certificación de la ACRN [3]. Con este certificado queda demostrada la pertenencia de la ACPA a la INCE y que cuenta con las correspondientes garantías de confianza. La ACPA se encuentra entonces subordinada a la ACRN y, al emitir certificados a los usuarios finales, actúa como eslabón intermedio en la “cadena de confianza”.

Debido al esquema en el cual se estructura la INCE, los PSCA que operan ACPA son las únicas Autoridad Certificadoras intermedias en la cadena de confianza. Esto significa que un PSCA no puede usar su ACPA para emitirle certificados a otra ACPA para que actúe como su subordinada.

De acuerdo con lo estipulado en la Política de Certificación de la ACRN [3], En ningún caso esta podrá emitir certificados a usuarios finales.

Un PSCA puede usar una misma ACPA para emitir certificados en base a distintas Políticas de Certificación siempre que cumpla con los requerimientos de cada una de ellas.

El PSCA debe elaborar para cada una de sus ACPA un documento denominado Declaración de Prácticas de Certificación, en el cual detalla los procedimientos técnicos y administrativos que implementa para cumplir con lo requerido por cada Política de Certificación a la cual adhiere. Este documento debe ser aprobado por la UCE previo a su puesta en práctica.

1.2.3. Autoridad de Registro

La Autoridad de Registro es la dependencia dentro del PSCA que atiende y procesa las solicitudes de emisión, renovación o revocación de certificados de parte del Suscriptor (punto 1.2.4). En este sentido, es el único punto de contacto requerido entre el PSCA y sus Suscriptores.

Como consecuencia de esto, la Autoridad de Registro es la responsable de la identificación de la persona física y quien da comienzo al procedimiento técnico de emisión, renovación o revocación de certificado.

La Autoridad de Registro hace entrega del certificado emitido al Suscriptor y le informa las buenas prácticas de uso. Debe, además, previo a la entrega del certificado, asegurarse que se firme el acuerdo con las Condiciones para la Utilización de Firma Electrónica Avanzada [4].

Las responsabilidades y acciones realizadas por la Autoridad de Registro se encuentran descriptas en la sección 2.1.3 de la presente Política de Certificación.

A su vez, cada PSCA debe detallar en su Declaración de Prácticas de Certificación las particularidades de funcionamiento de sus ACPA, las cuales deben estar alineadas con los requerimientos de la presente Política de Certificación.

1.2.4. Suscriptores

En el contexto de la presente Política de Certificación, los Suscriptores son personas jurídicas a quienes un PSCA a través de su ACPA les ha emitido certificados electrónicos de Persona Jurídica.

Si bien la responsabilidad por el uso del certificado es de la persona jurídica como suscriptor, en cualquier caso, el certificado es entregado a una persona física como referente del mismo, debidamente apoderada en el momento del registro. Los Suscriptores pueden utilizar certificados de Persona Jurídica con fines de autenticación, Firma Electrónica Avanzada y cifrado.

Los Suscriptores contraen derechos y obligaciones al utilizar certificados de Persona Jurídica según se describe en la presente Política de Certificación y normativa vigente

1.2.5. Terceros Aceptantes

En el contexto de la presente Política de Certificación, los Terceros Aceptantes son cualquier persona física u organización que confía en los certificados de la INCE para la autenticación o Firma Electrónica Avanzada de una persona jurídica (Suscriptor de un certificado de Persona Jurídica).

Los Terceros Aceptantes, al autenticar a una persona jurídica o al aceptar una Firma Electrónica Avanzada, están obligados a comprobar la validez del certificado. Para ello, deberán seguir los lineamientos estipulados en esta Política.

1.2.6. Otros participantes

No es aplicable.

1.3. Uso de los certificados

1.3.1. Usos Permitidos de los Certificados

Los usos habilitados para los certificados emitidos bajo la presente Política de Certificación de Persona Jurídica son los siguientes:

- a) Identificación y autenticación electrónica del Suscriptor del certificado (Persona Jurídica);
- b) Firma Electrónica Avanzada (según Ley N° 18.600, de 21 de Setiembre de 2009 [2]); y
- c) Cifrado de Datos.

1.3.2. Restricciones en el Uso de los Certificados

Los certificados emitidos por un PSCA bajo la presente Política de Certificación deben utilizarse de acuerdo con lo establecido en el punto 1.3.1, y a la normativa vigente.

1.4. Administración de la Política de Certificación

La administración de la presente Política de Certificación de Persona Jurídica es responsabilidad de la UCE.

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

Nombre: Unidad de Certificación Electrónica

Dirección de correo: info@uce.gub.uy

Teléfono: (+598) 2901 0065 opción 5

1.5. Relación entre la Política de Certificación y otros documentos

La presente Política de Certificación se basa en la Ley N° 18.600, de 21 de setiembre de 2009 [2] y en el correspondiente Decreto reglamentario N° 436/2011, de 8 de diciembre de 2011 [5], y prevalece sobre ella la legislación vigente y las disposiciones particulares adoptadas por la UCE.

Los requerimientos definidos en esta Política de Certificación deben ser instrumentados por los PSCA y especificados en su Declaración de Prácticas de Certificación.

Esta Política de Certificación tiene impacto en las Políticas de Seguridad de la Información y procedimientos administrativos asociados de las ACPA.

1.6. Procedimiento de Aprobación

La aprobación de esta Política, así como toda modificación introducida en ella, es responsabilidad exclusiva de la UCE. La UCE aplicará sus procedimientos internos de administración documental para garantizar la calidad y trazabilidad de los cambios realizados. La Política modificada se publicará como una nueva versión, manteniéndose un registro de la fecha y cambios realizados. Ver más información en la sección 8.

1.7. Definiciones y abreviaturas

Las definiciones y abreviaturas generales de la INCE se encuentran definidas en la Ley N° 18.600, de 21 de Setiembre de 2009 [2]. No obstante, las siguientes definiciones y

abreviaturas son utilizadas a lo largo del presente documento, y por lo tanto, son citadas también aquí.

Persona Jurídica (PJ): Según el inciso 2º del artículo 21 del Código Civil "Se consideran personas jurídicas y por consiguiente capaces de derechos y obligaciones civiles, el Estado, el Fisco, el Municipio, la Iglesia y las corporaciones, establecimientos y asociaciones reconocidas por la autoridad pública".

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

Prestador de Servicios de Certificación Acreditado (PSCA): persona física o jurídica acreditada ante la UCE y responsable de la operación de al menos una Autoridad Certificadora de la INCE.

Autoridad de Registro: en el contexto de la presente política, dependencia del PSCA responsable del registro y procesamiento de solicitudes de emisión, renovación y revocación de certificados, incluyendo la validación de la identidad de los suscriptores y/o de las solicitudes al inicio del proceso.

Autoridad Certificadora del Prestador Acreditado (ACPA): conjunto de sistemas, personal, políticas y procedimientos que el PSCA utiliza para emitir 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 la INCE estas políticas son promovidas, aprobadas y mantenidas por la UCE.

Certificado Electrónico (CE): documento electrónico firmado electrónicamente que da fe del vínculo entre el sujeto firmante o titular del certificado y los datos de creación de la firma electrónica.

Certificado Electrónico Reconocido (CER): Certificado Electrónico emitido por la ACRN o por un PSCA a través de una de sus ACPA.

Certificado Electrónico Reconocido de Persona Jurídica (CERPJ): Certificado Electrónico Reconocido cuyo suscriptor es una Persona Jurídica, emitidos en exclusividad por los PSCA y sujetos a los requerimientos de la presente Política de Certificación.

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

Solicitud de Firma de Certificado (CSR – Certificate Signing Request): en el contexto de la presente política, es un mensaje emitido por la organización a certificarse bajo el estándar PKCS#10 mediante el que solicita y provee información a una ACPA 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, o a un tercero especificado.

Dispositivo o Módulo Seguro de Creación de Firmas (DSCF): Dispositivo que resguarda las claves y el certificado de un suscriptor, utilizado para generar su firma electrónica y que, al menos, garantiza:

- a) Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;
- b) Que existe una expectativa razonable de que los datos utilizados para la generación de la firma no pueden ser descubiertos por deducción y la firma está protegida contra falsificación por medio de la tecnología disponible a la fecha, siendo posible detectar cualquier alteración posterior; y,
- c) Que los datos empleados en la generación de la firma pueden ser protegidos de modo fiable por el firmante legítimo, contra su utilización por terceros.

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.

Protocolo de Estado de Certificados Online (OCSP - Online Certificate Status Protocol): protocolo para la validación online del estado de revocación de certificados, de implementación opcional para los PSCA.

RSA (Rivest, Shamir y Adleman): Sistema criptográfico asimétrico, o “de clave pública”, utilizado para cifrado o para firmas electrónicas.

SHA (Secure Hash Algorithm - Algoritmo de Hash Seguro): Familia de funciones de *hash* (resumen) utilizadas como parte de la creación de firmas electrónicas. Dentro de esta familia se encuentran SHA-1, SHA-256 y SHA-512, entre otras.

NIST (National Institute of Standards and Technology): Agencia del Departamento de Comercio de los Estados Unidos de América.

LACNIC: El Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe. Es uno de los 5 Registros Regionales de Internet en el mundo.

Curva Elíptica: La Criptografía de Curva Elíptica (del inglés: Elliptic curve cryptography, ECC) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves más cortas que los métodos antiguos —como RSA— al tiempo que proporcionan un nivel de seguridad equivalente.

Curvas Edwards: En matemáticas, las curvas de Edwards son una familia de curvas elípticas estudiadas por Harold Edwards en 2007. El concepto de curvas elípticas sobre campos finitos se utiliza ampliamente en criptografía de curvas elípticas.

Curvas Brainpool: Son las curvas elípticas basadas en el RFC 5639.” Elliptic Cryptography (ECC) Brainpool Standard Curves and Curve Generation”

Curvas NIST: Refiere a las Curvas Elípticas definidas en el Standard RFC 6979 “Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)”.

2. Aspectos Generales de la Política de Certificación

2.1. Obligaciones

2.1.1. Obligaciones de la Unidad Reguladora

2.1.1.1. Obligaciones de la UCE

Las obligaciones de la UCE se encuentran especificadas en la Política de Certificación de la ACRN [3]. Además de dichas obligaciones generales, constituyen obligaciones específicas de la UCE en el contexto de la presente Política:

- a) La actualización, aprobación y cancelación de la presente Política de Certificación de la INCE – PKI Uruguay;
- b) La acreditación de Prestadores de Servicios de Certificación para operar dentro de la INCE emitiendo certificados de Persona Jurídica;
- c) La publicación de la lista de PSCA habilitados a emitir certificados de Persona Jurídica dentro del contexto de la INCE;
- d) Mantener a disposición permanente del público la presente Política de Certificación, tanto la versión vigente como las anteriores;
- e) Atender los pedidos de revocación de certificados de Persona Jurídica solicitados por una autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;

2.1.2. Obligaciones del Certificador

2.1.2.1. Obligaciones de la ACRN

Las obligaciones de la ACRN en el contexto de la presente Política son las mismas que se expresan en la Política de Certificación de la ACRN.

2.1.2.2. Obligaciones de los PSCA

En el contexto de la presente política, éstos son los PSC Acreditados por la UCE para la emisión de certificados de Persona Jurídica. Constituyen obligaciones de dichos Prestadores:

- a) Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, de conformidad con lo pautado en la presente Política;
- b) Generar la clave privada de sus ACPA con aprobación de la UCE, en presencia de personal de dicha Unidad y de la ACRN, y de acuerdo con los requerimientos del punto 6.2 de la presente Política;
- c) Proteger las claves privadas de sus ACPA;
- d) Solicitar la emisión del certificado de sus ACPA, de acuerdo con los procedimientos estipulados para tal fin en la Política de Certificación de la ACRN [3];
- e) Solicitar a la ACRN la revocación del certificado de sus ACPA ante sospecha real de compromiso de la clave privada asociada;
- f) Atender los requerimientos de revocación solicitados por la UCE o por los suscriptores, de acuerdo con la legislación vigente y con los procedimientos definidos en la presente Política;

- g) Utilizar el certificado de sus ACPA de acuerdo con los requerimientos de la presente Política de Certificación;
- h) La emisión, renovación y revocación de los certificados de Persona Jurídica de sus suscriptores;
- i) La emisión y publicación de su Lista de Certificados Revocados (CRL);
- j) Informar a sus suscriptores de la revocación de sus certificados, junto con la causal para dicha operación;
- k) El envío a la UCE de las CRL inmediatamente después de emitidas;
- l) Notificar a los suscriptores de los certificados emitidos por sus ACPA bajo la presente política, acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACPA y la emisión de un nuevo par de claves criptográficas, como también del procedimiento a seguir en ese caso;
- m) Garantizar el acceso permanente y gratuito de los suscriptores y Terceros aceptantes al sitio de publicación que contiene su propio certificado, y la lista de certificados revocados;
- n) Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad, no repudio o confidencialidad según corresponda)

2.1.3. Obligaciones de las Autoridades de Registro de los Prestadores Acreditados

Las obligaciones de las Autoridades de Registro de las ACPA, son asumidas por el PSCA, o por las instituciones que hayan sido mandatadas a estas instancias, y en el contexto de la presente Política son las siguientes:

- a) Recibir y procesar las solicitudes de emisión, renovación o revocación de certificados emitidos por la ACPA, de acuerdo con los requerimientos estipulados de la sección 4;
- b) Comprobar, de acuerdo con lo estipulado en el punto 3.1.2:
 - i. la identidad de la persona jurídica para la cual será emitido el certificado, a través de certificado notarial,
 - ii. la identidad de la persona física que solicita la emisión, renovación o revocación presencial del certificado, mediante la validación del documento de identidad presentado,
 - iii. que la persona cuente con las facultades necesarias para solicitar, renovar o revocar el certificado de la persona jurídica correspondiente
- c) Notificar a los suscriptores de certificados de Persona Jurídica emitidos por alguna de sus ACPA ante la ocurrencia de un evento que así lo requiera según lo estipulado por la presente Política de Certificación;

2.1.4. Obligaciones de los Suscriptores de Certificados

En el contexto de la presente Política de Certificación, los suscriptores son Personas Jurídicas constituidas en la República Oriental del Uruguay, bajo cuya responsabilidad recaerán las obligaciones citadas en este punto. Los certificados son emitidos a instancias de la solicitud de una persona física facultada para tal acto, que se convierte en el referente del mismo y del par de claves asociado. El referente puede solicitar unilateralmente su desvinculación del certificado, ante lo cual la Persona Jurídica deberá presentar un nuevo referente en un plazo máximo de 15 días hábiles, o de lo contrario el PSCA deberá proceder a la revocación del certificado. De la misma forma, la Persona Jurídica puede solicitar la asignación de un nuevo referente para un certificado propio, ante lo cual el antiguo referente queda automáticamente desvinculado del certificado en cuestión y no debería tener más acceso al mismo.

Toda la información necesaria para la identificación y autenticación de la Persona Jurídica a certificar, así como también de la Persona Física que lleva adelante el trámite de solicitud de certificado, debe ser provista de forma completa y precisa al iniciar el proceso de registro. Dicha información y procedimiento de registro se especifica en las secciones 3.1 y 4.1.

Al aceptar un certificado emitido por un ACPA de PSCA, la Persona Jurídica es responsable de toda la información por él provista y contenida en ese certificado, del buen uso del mismo, respetando la presente Política de Certificación y normativa vigente, y de la protección de la clave privada asociada.

La persona jurídica debe hacer uso del certificado en conformidad con la presente Política de Certificación para certificados de Persona Jurídica, con las demás Políticas de Certificación aplicables de la INCE y demás normativa vigente

Los Suscriptores de certificados de Persona Jurídica asumen las siguientes obligaciones:

- a) Proveer toda la información que le sea requerida de modo completo y preciso a la Autoridad de Registro a fines de obtener el certificado emitido por el PSCA a través de su ACPA bajo la presente política de certificación;
- b) Generar su clave privada en alguna de las condiciones establecidas en el punto 6.2.2;
- c) Proteger su clave privada;
- d) Solicitar la inmediata revocación del certificado emitido por el PSCA a través de su ACPA en el caso de compromiso o sospecha de compromiso de la clave privada asociada;
- e) Utilizar el certificado de acuerdo con los requerimientos de la presente política de certificación;

f) Cumplir con las obligaciones establecidas en la presente política de certificación, otras Políticas de Certificación aplicables de la INCE y otras reglamentaciones aplicables emitidas por la UCE;

g) Firmar las Condiciones para la Utilización de Firma Electrónica Avanzada [4] previo a la entrega del certificado por parte del PSCA.

2.1.5. Obligaciones de los Terceros Aceptantes

Los Terceros aceptantes tienen las siguientes obligaciones:

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

- i. garantías y usos aceptables del certificado de las ACPA de los PSCA;
- ii. garantías y usos aceptables de los certificados emitidos por los PSCA a Personas Jurídicas;
- iii. obligaciones de los Terceros aceptantes.

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

- i. se encuentra dentro de su período de vigencia,
- ii. su Firma Electrónica Avanzada puede ser verificada con el uso del mismo certificado de la ACRN, y
- iii. no ha sido revocado según la CRL publicada por la ACRN.

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

- i. se encuentra dentro de su período de vigencia,
- ii. su firma electrónica puede ser verificada con la clave pública del certificado de la ACRN, y
- iii. no ha sido revocado según la CRL publicada por la ACRN.

d) Verificar la validez del certificado de Persona Jurídica que le está siendo presentado. El certificado es considerado válido cuando:

- i. se encuentra dentro de su período de vigencia,
- ii. su firma electrónica puede ser verificada con la clave pública del certificado de la ACPA emisora, y
- iii. no ha sido revocado según la CRL publicada por dicha ACPA.

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

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

2.1.6. Obligaciones del servicio de repositorio de la INCE

El repositorio web público de la INCE no es un sitio único, sino que es la conjunción de los repositorios web públicos de todos los actores que la componen y publican información requerida por sus Políticas de Certificación, a saber: la UCE, la ACRN, los PSCA y otros actores determinados por resolución de la UCE.

La información que debe contener el repositorio web público de información de la UCE se encuentra especificada en la Política de Certificación de la ACRN [3]. Además, en el contexto de la presente Política publicará la siguiente información adicional:

- a) Esta Política de Certificación (versión vigente y anteriores);
- b) La lista de OIDs de la Declaración de Prácticas de Certificación de los PSCA que emiten certificados de Persona Jurídica;
- c) Información relevante de los informes de auditoría de la que fueron objeto los PSCA que emiten certificados de Persona Jurídica;
- d) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos designados por los PSCA que emiten certificados de Persona Jurídica, para la atención a suscriptores finales y Terceros aceptantes;

La información que debe contener el repositorio web público de información de la ACRN se encuentra especificada en la Política de Certificación de la ACRN [3]. Además, en el contexto de la presente Política deberá publicar la siguiente información adicional:

- a) Esta Política de Certificación (versión vigente y anteriores);
- b) Los certificados emitidos para ACPA que emitan certificados de Persona Jurídica.

Para esta Política de Certificación es obligatorio para todo PSCA que opere al menos una ACPA autorizada a emitir certificados de Persona Jurídica, el mantenimiento de un repositorio público de información, a través de un sitio web, que contenga la siguiente información:

- a) Todas las políticas de certificación (versiones vigentes y anteriores) que utilicen las ACPA del PSCA para la emisión de certificados, incluyendo ésta;
- b) La Declaración de Prácticas de Certificación de cada una de las ACPA del PSCA (versión vigente y anteriores);

- c) El Acuerdo con la ACRN que lo oficializa como suscriptor de Certificados de la ACRN;
- d) El certificado emitido por la ACRN para cada una de sus ACPA;
- e) La Lista de Certificados Revocados (CRL) de la ACPA;
- f) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos designados por el PSCA, para la atención a suscriptores finales y Terceros aceptantes;
- g) Referencia al sitio de publicación de información de la UCE;

2.2. Responsabilidades

En relación con la responsabilidad que pudiere imputarse a la ACRN o a la UCE, será de aplicación lo establecido en los artículos 24 y 25 de la Constitución de la República. Igual situación se verificará en caso de tratarse de una entidad pública que se acredite como PSCA.

En relación con la responsabilidad de los PSCA – entidad privada –, ésta será regulada de acuerdo con lo establecido en los artículos 1342 y 1344 del Código Civil, normas modificativas y complementarias.

2.3. Tarifas

Los PSCA que emitan certificados bajo la presente Política de Certificación podrán percibir una prestación económica por sus servicios.

2.4. Interpretación y aplicación de las normas

2.4.1. Legislación aplicable

La presente política deberá ser interpretada de acuerdo con lo establecido en la Ley N° 18.600, de 21 de Setiembre de 2009 [2], su normativa reglamentaria y las regulaciones aprobadas por la UCE. En igual sentido su validez, estructura y obligatoriedad derivan de la normativa legal, reglamentaria y regulatoria vigente.

2.4.2. Forma de interpretación y aplicación

En caso de conflictos en la interpretación de la presente política, la entidad competente a estos efectos es la Unidad de Certificación Electrónica, a la que podrá solicitársele el correspondiente dictamen.

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

2.4.3. Procedimientos de resolución de conflictos

Los suscriptores de certificados emitidos por los PSCA y los terceros aceptantes de dichos certificados podrán interponer una denuncia o una petición - según lo entiendan pertinente - ante la UCE en razón de conflictos relacionados con la prestación del servicio.

En todos los casos se encuentra habilitada la vía jurisdiccional correspondiente.

2.5. Publicación y Servicios de Estado de Certificados

2.5.1. Publicación de información del certificador

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

www.uce.gub.uy

Los PSCA, en su rol de Autoridades Certificadoras, deberán disponer de un sitio de publicación de información, cuya URL se deberá especificar en su Declaración de Prácticas de Certificación.

La información mínima que la UCE y los PSCA deben publicar en los sitios web se encuentra detallada en la sección 2.1.6.

2.5.2. Frecuencia de publicación

La UCE publicará información sobre políticas de certificación, acuerdos de privacidad y otros documentos relacionados con un máximo de cinco (5) días hábiles desde que se aprueben cambios. La información relativa a datos de contacto será actualizada con un máximo de cinco (5) días hábiles desde que se constaten cambios. Los PSCA deberán manejar los mismos plazos para ambos tipos de información, y deberán verificar y aprobar la misma en forma previa a la publicación.

El PSCA deberá actualizar la Lista de Certificados Revocados (CRL) de sus ACPA cuando ocurra al menos uno de los siguientes hechos:

- a) se produzca la revocación de un certificado, con un margen de tiempo de 2 horas luego de la revocación;

b) transcurran como máximo 24 horas luego de la última emisión de CRL.

El PSCA deberá especificar en su Declaración de Prácticas de Certificación los plazos reales que maneja y los mecanismos tecnológicos que implementa para cumplirlos, respetando siempre las cotas de tiempo presentadas en este punto.

2.5.3. Controles de acceso a la información

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

Los PSCA deberán brindar acceso irrestricto a toda la información que se publique en el repositorio público (ver punto 2.1.6) y establecer los controles necesarios para restringir la escritura o modificación de la información publicada.

2.5.4. Repositorios de certificados y listas de revocación

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

Los PSCA que emitan certificados bajo la presente Política deberán garantizar iguales niveles de servicio para su servicio de publicación de información.

2.6. Auditoría

Los requerimientos de auditoría de la UCE se encuentran estipulados en la Política de Certificación de la ACRN [3].

Los PSCA deberán someterse a auditorías periódicas de acuerdo con los lineamientos de la UCE. La información relevante de los informes de las auditorías deberá ser enviada a la UCE para su publicación en el sitio web de la Unidad, y deberá ser publicada en el sitio de publicación del PSCA.

2.7. Confidencialidad

A los efectos de la determinación del carácter de confidencialidad de la información se regulará de acuerdo con el marco normativo vigente.

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

2.7.1. Publicación de Información sobre los PSCA

La información que la UCE publica sobre los PSCA se encuentra estipulada en la Política de Certificación de la ACRN [3].

2.7.2. Publicación de Información sobre los Suscriptores Finales

Los PSCA no deberán publicar información alguna acerca de sus suscriptores de certificados, salvo la información contenida en los certificados mismos.

2.7.3. Publicación de Información sobre Revocación de Certificados

La información sobre la revocación de los certificados de persona jurídica, no se considera confidencial y será publicada por los PSCA mediante las CRL de sus ACPA. La dirección concreta de publicación deberá ser especificada en su Declaración de

Prácticas de Certificación. Las razones que dan lugar a la revocación se consideran públicas, y estarán incluidas en la CRL misma de acuerdo con la codificación estándar.

Dichas CRL serán enviadas a la UCE para su conocimiento y publicación de acuerdo con lo establecido en el punto 2.1.1.

2.7.4. Divulgación de información a autoridades judiciales

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

2.7.5. Divulgación de información por solicitud del suscriptor

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del suscriptor o de cualquier otra información generada o recibida durante el ciclo de vida del certificado solo se hará efectiva previa autorización del titular.

2.7.6. Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales la UCE divulgue o que el PSCA esté autorizado a divulgar información.

2.8. Derechos de propiedad intelectual

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

3. Identificación y Autenticación

3.1. Registro inicial

Podrán solicitar certificados de Persona Jurídica en el marco de la INCE, Personas Jurídicas legalmente constituidas o reconocidas en la República Oriental del Uruguay.

Para solicitar la emisión de un certificado de Persona Jurídica, deberá presentarse ante la Autoridad de Registro del PSCA una persona física con la documentación que acredite su identidad, la documentación que acredite la identidad de la persona jurídica y la documentación que acredite que está autorizado por ésta a realizar la operación.

La Autoridad de Registro del PSCA validará la autenticidad de la documentación presentada, así como también la identidad de la persona que solicita el registro y de la persona jurídica para la cual lo solicita, de acuerdo con los requerimientos de validación para cada uno de los documentos presentados.

3.1.1. Nominación

Una vez validada la constitución de la persona jurídica, la identidad del representante y su legitimación para realizar la solicitud, los datos que se colocarán en el certificado serán los datos de la persona jurídica, de la forma que figura en el certificado notarial que la identifica.

3.1.1.1. Formato del Nombre Distinguido

Para el nombre de la Persona Jurídica se deberá utilizar el campo “Subject” del certificado emitido a través de la ACPA (ver sección 7.1). El formato para indicar el nombre deberá ser X.500 (Distinguished Name).

Dicho formato, se aplicará de la siguiente forma:

Country (C): UY (Uruguay según la nomenclatura ISO 3166-1)

Common Name (CN): Nombre de fantasía de la persona jurídica, tal y como está escrito en el certificado notarial presentado y usando sólo letras mayúsculas.

Organization (O): Nombre de la persona jurídica, tal y como está escrito en el certificado notarial presentado y usando sólo letras mayúsculas.

serialNumber: tipo de registro, según se identifique la organización en el certificado notarial, más el número.

Los tipos de registros aceptados son Registro Único Comercial en la Dirección General Impositiva, identificado mediante la sigla RUC (Registro Único Tributario), registro en el Banco de Previsión Social, identificado mediante la sigla BPS, y registro en la Dirección General de Registro del Ministerio de Educación y Cultura, identificado mediante la sigla DGR.

Por mayor detalle acerca de la nominación y formatos de los nombres, referir a la sección 7.

A modo de ejemplo, para la empresa “EMPRESA S.A.”, con nombre de fantasía “La Empresa” e inscrita en DGI con RUC 010328960013, su nombre distinguido para el certificado de persona jurídica se conformaría de la siguiente manera:

C=UY

CN=LA EMPRESA

O=EMPRESA S.A.

serialNumber=RUC010328960013

3.1.2. Validación inicial de identidad

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

3.1.2.1. Identidad

La persona física que solicita efectivamente el certificado deberá demostrar en primera instancia su propia identidad ante la Autoridad de Registro del PSCA, presentando el documento de identificación correspondiente, cédula de identidad uruguaya o pasaporte, vigentes y en buen estado.

Luego de eso, el individuo deberá demostrar la existencia de la persona jurídica a la cual representa en este acto, presentando certificado notarial de la misma, con no más de 30 días desde su emisión.

Finalmente, el individuo deberá acreditar su representación para solicitar el certificado en nombre de la persona jurídica.

3.1.2.2. Clave Privada

Las claves privadas asociadas a certificados de Persona Jurídica emitidos bajo la presente Política deberán ser siempre generadas y utilizadas en un Dispositivo o Módulo Seguro de Creación de Firmas (DSCF) de hardware o de software.

Para la emisión del certificado bajo la presente Política de Certificación, el PSCA debe verificar que la llave privada correspondiente a la llave pública del CSR (Certificate Signing Request) esté en posesión de la persona física que está solicitando el certificado y sea la misma utilizada para firmarlo. La persona física que solicita el certificado se convierte en el referente del mismo, y del par de claves asociado. El PSCA deberá registrar internamente esta asociación entre la persona jurídica suscriptora y la persona física referente del certificado.

3.1.3. Identificación y autenticación para solicitudes de cambio de clave

El procedimiento de cambio de clave es el de Emisión de Certificado, por lo que se aplica lo mismo que para el punto 3.1.2.

3.1.4. Identificación y autenticación para solicitudes de desvinculación de referente

La persona física que actúa como referente del certificado de persona jurídica, puede en cualquier momento solicitar su desvinculación del mismo en forma unilateral. Para esto, deberá concurrir en forma presencial a la Autoridad de Registro del PSCA y solicitar la desvinculación del certificado.

El PSCA deberá validar la identidad de la persona física de igual forma que para la solicitud de emisión (punto 3.1.2), y verificar que efectivamente es la persona física referente del certificado. Una vez realizada esta validación, el PSCA realizará la desvinculación, y notificará a la persona jurídica suscriptora de este hecho de forma urgente. A partir de este momento, las responsabilidades del antiguo referente para con el certificado de persona jurídica cesan completamente.

Si la Persona Jurídica suscriptora no presentase un nuevo referente en los próximos 15 días hábiles, el PSCA deberá proceder a la revocación del certificado en forma automática, volviendo a notificar al PSCA de este hecho.

3.1.5. Identificación y autenticación para solicitudes de vinculación de referente

La persona física que lleva adelante la solicitud del certificado de persona jurídica queda registrada como referente del mismo en forma automática. Sin embargo, en la eventualidad que este se desvincule del mismo, de acuerdo con lo estipulado en el punto 3.1.4, la persona jurídica deberá presentar un nuevo referente en un plazo no mayor a 15 días hábiles, o de lo contrario su certificado deberá ser revocado.

De la misma manera, la Persona Jurídica suscriptora puede solicitar un cambio de referente. Al completar el procedimiento de vinculación del nuevo referente, como se describe a continuación, el anterior referente queda automáticamente desvinculado del certificado.

En cualquiera de los dos casos, para presentar un nuevo referente, se debe realizar el mismo proceso que para la solicitud original de acuerdo al punto 3.1; solamente el registro, no la generación de claves ni emisión del certificado, puesto que se está utilizando el mismo.

3.1.6. Identificación y autenticación para solicitudes de revocación

Las personas jurídicas que cuenten con un certificado emitido por un PSCA podrán solicitar la revocación del mismo. La revocación de un certificado es un proceso por el cual se termina prematuramente su período de validez, y se realiza cuando se detecta un mal uso del certificado o se sospecha de compromiso de su clave privada asociada, entre otros. Las causales de revocación se detallan en el punto 4.11.1.

Para la solicitud presencial, la persona deberá presentarse ante la Autoridad de Registro del PSCA presentando la misma documentación que para el registro inicial (ver 3.1.2); debe estar apoderada para solicitar revocación en lugar de emisión. En el caso de certificados de persona jurídica, dicha solicitud puede entonces ser realizada por cualquier persona física que figure como representante legal en el certificado notarial presentado o esté debidamente apoderada para realizar esta solicitud.

La revocación deberá realizarse en forma inmediata una vez comprobada la autenticidad de la solicitud. Una vez validada la identidad de la Persona solicitante, así como su autorización para revocar y procesada la solicitud, el PSCA cuenta con un plazo máximo de 2 horas para emitir y publicar una nueva CRL que contenga dicho certificado, y para actualizar sus servicios OCSP, si es que dispone de ellos.

4.Requerimientos Operativos del Ciclo de Vida de los Certificados

En el presente capítulo, se refiere a la persona jurídica titular del certificado electrónico como “Suscriptor” o “Suscriptora”, mientras que el individuo que lleva adelante el trámite de solicitud y queda como referente del certificado y del par de claves es llamado “Solicitante” o “Referente”, según se trate del proceso de solicitud o no.

4.1.Solicitud de certificado

4.1.1. Legitimación para solicitar la emisión

Podrá solicitar un certificado de Persona Jurídica toda persona jurídica constituida o reconocida en la República Oriental del Uruguay, que cuente con registro en la Dirección General Impositiva (RUC – Registro Único Comercial), en el Banco de Previsión Social (número de BPS) o en la Dirección General de Registro del Ministerio de Educación y Cultura (registro en la DGR). La identidad de la persona jurídica debe demostrarse mediante certificado notarial que contenga alguno de estos tipos de registro, junto con el número correspondiente. El certificado notarial no debe tener más de 30 días de emitido al momento de su presentación para el registro.

Para la solicitud efectiva del certificado, podrá actuar toda persona ciudadana uruguaya o del extranjero, mayor de edad, que presente Cédula de Identidad Uruguaya o Pasaporte. El documento de identidad debe ser original, encontrarse vigente y en buenas condiciones al momento de presentarlo ante la Autoridad de Registro del PSCA. Además, deberá ser representante legal de la persona jurídica, según lo indique el certificado notarial, o contar con un poder específicamente certificado por escribano público para este fin.

4.1.2. Registro de las solicitudes de certificados

La solicitud de certificado puede iniciarse de forma presencial o remota (web, mail, etc.) según lo determine cada PSCA. En cualquier caso, el PSCA debe documentar la solicitud de certificado y dar comienzo a sus procedimientos internos de emisión, según lo deberá describir en su Declaración de Prácticas de Certificación.

El procedimiento de solicitud de certificado debe contar con una instancia presencial donde se valide la identidad del individuo solicitante (previo a la emisión del certificado), según lo especifica la sección 3.1.2 de esta Política de Certificación.

Además de la identidad del individuo solicitante, la Autoridad de Registro del PSCA debe validar la identidad de la persona jurídica mediante el certificado notarial correspondiente, y validar que el individuo cuenta con las facultades necesarias para solicitar un certificado para la persona jurídica, sea porque es representante legal de la misma o porque cuenta con un poder que así lo acredita.

Queda a criterio de cada PSCA la documentación adicional requerida para la solicitud del certificado.

El individuo que lleva adelante la solicitud del certificado deberá generar el par de claves de acuerdo con los requerimientos técnicos de la sección 6.2.2. Una vez generado el par de claves, deberá generar un CSR firmado y enviarlo a la Autoridad de Registro del PSCA en forma segura para la emisión del certificado.

En caso de que la generación sea realizada en instalaciones del PSCA o a través de un servicio web, éste no deberá almacenar copia de la clave privada ni del PIN que la protege en ningún soporte.

Independientemente del mecanismo, el par de claves debe ser generado en un DSCF de hardware o software protegido por, al menos, un PIN. El PSCA deberá informar al Solicitante la importancia que tiene la protección de la clave privada, así como dar pautas para un almacenamiento y uso seguros.

Como parte del proceso de solicitud de certificado, el solicitante debe firmar las Condiciones para la Utilización de Firma Electrónica Avanzada [4]. Este acuerdo, elaborado por el PSCA, registra la adhesión del solicitante a la presente Política de Certificación y a la regulación aplicable emitida por la UCE. En caso de que el Solicitante no firme este Acuerdo, no se puede continuar con el proceso de emisión de un certificado.

4.2. Procesamiento del requerimiento de certificado

Una vez que la Autoridad de Registro del PSCA registró la solicitud de certificado – según se especifica en la sección 4.2-, el PSCA a través de su ACPA debe autorizar la emisión del certificado.

En el caso de que el PSCA opere de forma independiente la Autoridad de Registro y la ACPA, debe implementar un mecanismo que asegure la integridad y autenticidad de la información asociada con los certificados y que se transmite de un sitio a otro.

En ningún momento, durante el procesamiento de la solicitud de certificado, el PSCA puede acceder a la clave privada del Suscriptor ni al PIN que la protege.

El plazo entre el registro de solicitud de un certificado (dado por la validación presencial de la identidad del Solicitante y la validación del resto de la documentación requerida) y la entrega del certificado al Suscriptor no puede exceder los 10 días hábiles.

4.3. Emisión de certificado

En caso de que el PSCA reciba en su ACPA el CSR ya generado, debe realizar las verificaciones correspondientes de autenticidad, integridad, exactitud de la información contenida y autorización en forma previa a la emisión del certificado. Los procedimientos para estas verificaciones se deberán documentar en la Declaración de Prácticas de Certificación de cada ACPA de PSCA.

El PSCA debe ejecutar sus procedimientos internos de emisión de certificado y asegurar durante los mismos el cumplimiento de las condiciones de seguridad requeridas en la sección 5 de esta Política.

El período máximo de vigencia de un certificado es de 2 años. Un certificado debe entrar en vigencia en un período menor a 5 días hábiles a partir de la fecha en que es emitido.

Una vez que el certificado ha sido generado, el PSCA deberá notificar al Suscriptor en un plazo menor a 1 día hábil. Las vías de notificación y entrega de los certificados emitidos deberán ser detalladas en la Declaración de Prácticas de Certificación del PSCA. Si el Solicitante o el Suscriptor no confirman la recepción del certificado en un plazo de 30 días calendario, el PSCA deberá proceder a la revocación del mismo y notificar de este hecho al Solicitante y a la persona jurídica Suscriptora.

4.4. Aceptación de certificado

Una vez que el certificado es entregado al Solicitante, éste debe verificar la exactitud de la información de la persona jurídica que éste contiene.

En caso de que exista un error en la información del certificado, el Solicitante deberá notificar al PSCA para que revoque el certificado de forma inmediata (ver plazos de revocación en la sección 4.1.4 de esta Política). La emisión de un nuevo certificado, así como las condiciones, plazos y aranceles para esta operación, son determinados por el PSCA y deben ser especificados en su Declaración de Prácticas de Certificación.

Aunque el Suscriptor del certificado sea la persona jurídica, la persona física solicitante quedará registrada como referente del mismo.

4.5. Uso del Certificado y del Par de Claves

La persona jurídica Suscriptora puede utilizar el certificado y su par de claves únicamente para los fines descritos en la sección 1.3 de esta Política de Certificación.

El Suscriptor no podrá hacer uso del certificado ni de su clave privada sin que el Solicitante haya firmado previamente las Condiciones para la Utilización de Firma Electrónica Avanzada [4].

El Suscriptor será responsable por el uso y custodia de la clave privada asociada al certificado.

En caso de que el Suscriptor sospeche del compromiso de la clave privada, debe solicitar la revocación inmediata del certificado al PSCA. (Ver 4.11.1).

El Tercero Aceptante, para hacer uso de un certificado, tendrá la carga de realizar las siguientes comprobaciones:

- a) El certificado es válido y fue emitido por un PSCA de la INCE;
- b) El certificado se está utilizando para uno de los usos permitidos en esta Política de Certificación (ver 1.3);
- c) El certificado no se encuentra revocado en la última CRL emitida por el PSCA al momento de la validación, o el servicio de validación online OSCP provisto por el PSCA lo reporta como válido;
- d) El certificado del PSCA emisor es válido de acuerdo con la Política de Certificación de la ACRN, y
- e) El certificado de la ACRN es válido.

4.6. Renovación del certificado

La renovación de un certificado consiste en la emisión de un nuevo certificado. Este nuevo certificado puede mantener el par de claves utilizado por el certificado a renovar. Este servicio será opcional y a criterio del Prestador de Servicios de Certificación Acreditado.

El nuevo certificado debe contener los mismos datos que el certificado original. En el caso que se requiera modificar estos datos, la renovación no es un procedimiento válido. Referirse a la sección 4.8 para más información.

La validez de los certificados deberá ser, como máximo, de dos años, y están permitidas un máximo de dos renovaciones. El objetivo es que el período de validez del par de claves de un certificado no sea, en ningún caso, superior a los 6 años (emisión original de dos años y dos renovaciones de dos años cada una).

El certificado renovado debe entrar en vigencia en fecha igual o posterior a la de expiración del certificado actual del Solicitante.

En el caso de la renovación, se puede iniciar el trámite en un período que va desde 1 mes previo a la fecha de vencimiento. Los PSCA no deberán aceptar solicitudes de renovación fuera de este intervalo de tiempo.

El Solicitante debe autenticar su solicitud de renovación de forma idéntica a la solicitud original, conforme lo requiere el punto 4.1 de esta Política. En caso de que sea una persona física diferente al referente actual quien realiza la renovación, el PSCA deberá automáticamente cambiar al nuevo referente por el anterior, que queda desvinculado del certificado.

El procedimiento para autenticación de solicitudes de renovación deberá ser especificado en detalle en su Declaración de Prácticas de Certificación.

4.7. Cambio de Clave del Certificado

El procedimiento que aplica al cambio de clave de un certificado es el de Emisión de Certificado.

4.8. Modificación del certificado

La modificación de un certificado no es una operación permitida. Deben en su lugar aplicarse los procedimientos de Revocación y Emisión de Certificado, en el respectivo orden.

4.9. Desvinculación del referente del certificado

Para la desvinculación como referente del certificado, la persona física debe realizar la solicitud en forma presencial ante la Autoridad de Registro del PSCA y demostrar su identidad de la misma forma que para el registro inicial (ver punto 3.1.2).

El PSCA deberá verificar la identidad de la persona física, y verificar que efectivamente es el referente del certificado del cual se desea desvincular. Una vez realizada la validación, el PSCA procede a registrar su desvinculación, y a notificar a la Persona Jurídica Suscriptora en forma urgente.

La persona jurídica suscriptora cuenta con un plazo de 15 días hábiles para presentar un nuevo referente, o de lo contrario el PSCA deberá proceder a revocar su certificado, notificando nuevamente al Suscriptor en este caso.

4.10. Vinculación de un nuevo referente del certificado

En caso de desvinculación del referente de un certificado, la persona jurídica cuenta con 15 días hábiles para la presentación de un nuevo referente para el mismo en la Autoridad de Registro del PSCA, o de lo contrario su certificado será revocado por el PSCA. De la misma forma, la persona jurídica puede presentar un nuevo referente por iniciativa propia para sustituir al anterior. En este caso, una vez registrado el nuevo referente para el certificado de la persona jurídica, el anterior queda automáticamente desvinculado del mismo.

En cualquier caso, el registro de un nuevo referente debe realizarse de forma idéntica al registro inicial para la solicitud del certificado (ver 4.1), pero sin generación de claves

ni emisión de certificado, solo el registro certificado-referente que el PSCA mantendrá internamente.

4.11.Revocación y suspensión del certificado

La suspensión de un certificado no es una operación permitida.

4.11.1. Causas para la revocación

Las causas de revocación de un certificado son las siguientes:

- a) solicitud de representante legal del Suscriptor;
- b) vencimiento del plazo de 15 días hábiles para presentar un nuevo referente una vez desvinculado el anterior;
- c) pérdida, sospecha de compromiso o destrucción del soporte donde se encuentra almacenada la clave privada del certificado;
- d) pérdida, sospecha de compromiso o destrucción de la clave privada del certificado;
- e) datos erróneos o inexactos en el certificado;
- f) disolución de la persona jurídica Suscriptora;
- g) revocación de la ACPA del PSCA que emitió el Certificado;
- h) resolución judicial que así lo determine;
- i) otros.

Si el PSCA requiere la revocación del certificado por la causal “otros”, deberá comunicarse con la UCE, la que adoptará una resolución.

En caso de identificarse una de estas causales de revocación, deberá iniciarse el procedimiento de revocación de inmediato.

4.11.2. Legitimación para solicitar la revocación

Se encuentran habilitados a solicitar al PSCA la revocación de un certificado, justificando el cumplimiento de una de las causales de revocación mencionados en la sección 4.11.1, los siguientes actores:

- a) un representante legal del Suscriptor,
- b) el mismo PSCA; y,
- c) la UCE.

4.11.3. Procedimiento de revocación

La solicitud de revocación de un certificado debe realizarse ante la Autoridad de Registro del PSCA en forma presencial, la cual debe contar con atención al público para recibir solicitudes de revocación de certificados al menos durante 6 horas diarias, en días hábiles, entre las 8 y las 20 horas.

La solicitud de revocación requiere la autenticación del solicitante, y en cualquier situación de revocación, el PSCA deberá confirmar al Suscriptor la revocación una vez efectivizada la misma.

El PSCA deberá establecer y publicar cuáles de los puestos de atención al público de sus Autoridades de Registro son capaces de recibir solicitudes de revocación de

certificados de persona jurídica. El PSCA deberá realizar las mismas verificaciones de identidad de la persona física, de la persona jurídica y las facultades que la primera tiene para solicitar la revocación, de forma análoga a cómo se realiza en el caso de la emisión de certificado (Ver sección 4.1).

En todos los casos, la comunicación de la solicitud de revocación entre la Autoridad de Registro y la ACPA debe autenticarse y validarse su integridad.

4.11.4. Plazo máximo de procesamiento de 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.

4.11.5. Comprobación del estado de revocación de un certificado

Para la validación de un certificado (ver sección 2.1.5), el Tercero Aceptante podrá consultar el estado de revocación del certificado a través de la CRL en él especificada. Esta CRL se encontrará en el Repositorio de Información del PSCA emisor del certificado.

El PSCA, a través de su ACPA debe emitir una nueva CRL cada un período máximo de 2 días, en caso de no haber necesitado emitir una CRL por revocación de certificado.

Opcionalmente, los PSCA podrán implementar servicios de validación de estado OCSP. Estos servicios son adicionales a la CRL, y en caso de proveerlos, deberán documentar su mecanismo de uso en su CPS, y proveer las URL de consulta en la misma.

4.12. Servicios de estado del certificado

Para la comprobación del estado de un certificado, los PSCA deben implementar obligatoriamente el mecanismo de CRL.

Los PSCA deberán publicar en su Repositorio de Información el histórico de CRL emitidas para su consulta gratuita e irrestricta.

Debe encontrarse dentro del Repositorio, en la misma URL que se especifica en el perfil del certificado (sección 7.1), la última versión de CRL.

El PSCA deberá garantizar alta disponibilidad de la información, a excepción de los períodos planificados de mantenimiento.

Los PSCA podrán implementar otros mecanismos de validación de estado de revocación de certificados, como OCSP, pero ninguno de éstos puede sustituir a la CRL como mecanismo obligatorio.

4.13. Fin de la suscripción

El fin de la suscripción ocurre en las siguientes situaciones:

- a) El certificado alcanzó su fecha de expiración;
- b) El certificado fue revocado por el PSCA previo a alcanzarse su fecha de expiración; o,
- c) El certificado del PSCA emisor fue revocado por la ACRN.

4.14. Archivado y recuperación de clave

No se encuentra permitido realizar archivado (*escrow*) de la clave del Suscriptor para certificados de persona jurídica.

5. Controles de Seguridad Física, de Procedimiento y de Personal

Con respecto a los Controles de Seguridad Física, de Procedimiento y de Personal, los PSCA deberán cumplir con los requerimientos técnicos especificados en la resolución N° 06/2011 de la UCE, de 28 de diciembre de 2011. Sin perjuicio de esto, se describen en la presente sección otros controles administrativos, operativos y físicos que también deben implementar los PSCA para la protección de la información asociada con sus operaciones y a los certificados emitidos, tanto desde el punto de vista de la confidencialidad, como de la integridad, el no repudio y la disponibilidad.

Se entiende, como parte de esta información, entre otros:

- a) la información de la Persona Jurídica;
- b) la información personal del referente actual y anteriores si hubiese;
- c) los trámites de solicitud, renovación o revocación de certificados;
- d) la clave privada del certificado emitido –en caso de que la generación la realice el PSCA-;
- e) los documentos internos del PSCA, que describen los procesos operativos y los controles de seguridad implementados;
- f) los registros de auditoría impresos o en sistemas informáticos; y,
- g) las Condiciones para la Utilización de Firma Electrónica Avanzada [4] y Declaración de Prácticas de Certificación del PSCA.

Los objetivos de control mencionados en esta sección aplican tanto a las instalaciones de producción como de respaldo de las ACPA.

El PSCA debe incluir un resumen de los procedimientos de control en su Declaración de Prácticas de Certificación y debe documentarlos en detalle en sus procedimientos internos.

Los procedimientos internos del PSCA, así como los registros generados durante su aplicación, serán auditados por la UCE.

5.1. Controles de seguridad física

Los PSCA deberán implementar sólidas medidas de seguridad física para la protección del equipamiento e instalaciones de sus ACPA, tanto de accesos no autorizados como de siniestros como incendios e inundaciones.

Mínimamente se deben implementar los siguientes controles:

- a) Controles para el acceso físico del personal a las instalaciones;
- b) Definición de perímetros de seguridad en función de la criticidad de la información;
- c) Inventario de activos físicos de información y controles periódicos de inventario;
- d) Controles para el ingreso y egreso de activos físicos de información;
- e) Controles para la protección de la infraestructura contra incendios e inundaciones;
- f) Controles para la protección contra factores climáticos tales como humedad y temperatura;
- g) Procedimiento para disposición de información.

5.2. Controles procedimentales

Los procesos que permiten el funcionamiento de la ACPA deberán estar documentados y basarse en la contraposición de intereses para las operaciones más críticas.

Cada PSCA deberá definir al menos los siguientes roles para la operación de sus ACPA:

- a) Custodio de clave;
- b) Oficial de Seguridad; y,
- c) Administrador de Sistemas.

Quienes desempeñen el rol de Custodio de clave tienen asignada la responsabilidad de proteger la clave privada de la ACPA, tanto su copia de producción como su copia de respaldo.

Por esta razón, este rol debe ser ejercido por personas de confianza del PSCA, seleccionadas de acuerdo con los procedimientos descriptos en la sección 5.3. Los Custodios de clave deben firmar con el PSCA un contrato de responsabilidad al asumir el rol.

Los custodios de clave participarán en la activación de la clave privada de la ACPA. Se entiende por procedimiento de activación de la clave privada, el procedimiento necesario para que la ACPA pueda realizar emisiones de certificados y CRL. Para este procedimiento, se requiere conocimiento dividido y contraposición de intereses. Esto significa que la clave privada no podrá ser activada únicamente por un custodio, sino que se requerirá un mínimo de dos. Las ACPA podrán implementar un esquema del tipo M de N para la activación de la ACPA. En este esquema, se requerirán M custodios cualesquiera, con M mayor o igual a 1, de los N totales, mayor o igual a 2, para activar la ACPA. En cualquier caso, el PSCA será responsable porque siempre exista un conjunto de custodios de clave disponibles para activar la ACPA.

Un custodio de clave puede desempeñar otros roles, siempre y cuando se respete el esquema M de N al momento de operar con la clave privada de la ACPA.

Quienes desempeñen el rol de Oficial de Seguridad deberán revisar los registros generados durante la aplicación de los procedimientos internos de la ACPA. En esta revisión, deberán comprobar la aplicación de los controles y medidas de seguridad estipulados. A su vez, deberán contrastar estos registros con aquéllos de auditoría de los sistemas de información e informar en caso de existir datos que no se correspondan.

El Oficial de Seguridad no puede participar con otro rol en los procedimientos que revisa.

El Administrador de Sistemas es el responsable de implementar las medidas y controles técnicos de seguridad en los sistemas de información de la ACPA.

5.3. Controles de seguridad del personal

Los individuos que desempeñan un rol de confianza deben ser seleccionados de acuerdo con procedimientos que verifiquen sus referencias, antecedentes laborales y valores éticos y profesionales.

Mínimamente se deben implementar los siguientes controles:

- a) Ingreso de personal (políticas de selección, evaluación e inducción);
- b) Cambio de rol de la persona (asignación de permisos, cambio de privilegios de su cuenta de usuario, firma de contrato de confidencialidad o responsabilidad, etc.);
- c) Capacitación del personal (capacitación inicial y capacitaciones periódicas por rol, material utilizado para capacitación, planes de entrenamiento);
- d) Retiro temporal o definitivo del personal (bloqueo o eliminación de sus cuentas de usuario);
- e) Políticas para el trabajo de personal contratado (externo a la ACPA);

f) Política de sanciones para incumplimiento de las normas de seguridad de la ACPA (acceso no autorizado, uso inadecuado de los sistemas, uso indebido de privilegios, etc.).

5.4. Controles para registros de auditoría

Estos controles deben ser implementados con el objetivo de registrar los eventos sucedidos. De esa manera puede realizarse un monitoreo continuo y la eventual reconstrucción de los eventos en caso de un incidente de seguridad. Es clave la protección de la integridad y disponibilidad de los registros generados.

Se deben implementar como mínimo los siguientes controles:

Se deben registrar todas las actividades realizadas por individuos o por sistemas informáticos durante el ciclo de vida de los certificados:

- a) registro y procesamiento de solicitudes;
- b) emisión, renovación y revocación de certificados en la ACPA;
- c) generación de la clave privada -en caso de que aplique-;
- d) Firma de las Condiciones para la Utilización de Firma Electrónica Avanzada [4].

Los registros relativos a la validación de solicitudes y a la generación de claves, así como aquéllos relativos a la información contenida en los certificados de los suscriptores y los certificados mismos deberán ser almacenados por un período compatible con las disposiciones normativas vigentes en materia de prescripciones.

Los registros deben ser protegidos contra su eliminación o modificación implementando medidas administrativas y técnicas de control de acceso. El Oficial de Seguridad debe asumir la responsabilidad de su protección y deben adoptarse esquemas de contraposición de intereses en caso de ser necesario.

Deben implementarse procedimientos de respaldo de los registros de auditoría y deben protegerse estos respaldos con los mismos requerimientos de seguridad que los registros originales.

Deben implementarse procedimientos para la revisión periódica de registros y detección de anomalías o incidentes de seguridad.

5.5. Procedimiento para el cambio de certificado de la ACPA

Según la Política de Certificación de la ACRN [3], una ACPA de PSCA no puede emitir certificados que expiren en una fecha posterior a la de expiración de su propio certificado. En su lugar, el PSCA debe solicitar un nuevo certificado para su ACPA a la ACRN. Este procedimiento se encuentra detallado en la sección 4.6 de la citada Política.

5.6. Procedimientos para recuperación de desastres

Deben establecerse procedimientos que permitan la recuperación de los sistemas, continuidad de las operaciones y la protección de la información en caso de que ocurra un desastre o compromiso de un sistema o clave. Es especialmente crítica la continuidad de los servicios de revocación de certificados y publicación de CRL (ver sección 2.5).

Deben abordarse mínimamente los siguientes requerimientos:

- a) Políticas para identificación de incidentes que puedan ocasionar un desastre en la operativa de la ACPA;
- b) Procedimientos de recuperación para infraestructura y software en el caso de corrupción de datos;
- c) Procedimientos para actuar en el caso de que la clave privada de la ACPA haya sido comprometida o se sospeche de su compromiso;

d) Procedimientos para la protección de la información y continuidad de las operaciones en el caso de un desastre natural (inundación, incendio, derrumbe, etc.).

5.7. Procedimientos para terminación de las operaciones

En el contexto de la presente política, se entiende por terminación de operaciones tanto la terminación total de una ACPA, como la discontinuación de certificados de Persona Jurídica. En ambos casos, los PSCA deberán realizar la terminación de las operaciones de sus ACPA de acuerdo con las regulaciones establecidas por la UCE.

6. Controles de Seguridad Técnica

Con respecto a los Controles de Seguridad Técnica, los PSCA deberán cumplir con los requerimientos técnicos especificados en las resoluciones de la UCE. Sin perjuicio de esto, se describen en la presente sección otros controles que también deben implementar los PSCA, específicamente para la seguridad en la gestión de claves privadas y certificados.

6.1. Instalación del equipamiento informático de la ACPA

Los requisitos que el PSCA debe cumplir para la instalación del equipamiento informático de la ACPA se encuentran en la sección 6.1.2 de la Política de Certificación de la ACRN [3].

6.2. Generación e instalación del par de claves

6.2.1. Generación e instalación del par de claves de la ACPA

Los requisitos que el PSCA debe cumplir para la generación e instalación del par de claves de una ACPA se encuentran en la sección 6.2.2 de la Política de Certificación de la ACRN [3].

6.2.2. Generación del par de claves para Persona Jurídica

El par de claves debe ser siempre generado en un Dispositivo Seguro de Creación de Firmas (DSCF) de hardware o software, en poder de la persona física solicitante (referente), y la clave privada debe ser mantenida y utilizada con este dispositivo bajo el

control de la persona jurídica suscriptora. En caso de solicitudes completamente presenciales, está permitida la generación en instalaciones del PSCA.

El par de claves generado debe ser RSA y tener un largo mínimo de 2048 bits.

Una vez generado el par de claves, el individuo solicitante debe enviar el CSR conteniendo la clave pública al PSCA mediante un canal seguro, que garantice su integridad.

La clave privada del certificado de Persona Jurídica puede ser utilizada para autenticar a la persona jurídica, firmar electrónicamente y cifrar información. Ver sección 4.5.

6.3. Protección de la clave privada

6.3.1. Protección de la clave privada de la ACPA

Los requisitos que el PSCA debe cumplir para la protección de la clave privada de la ACPA se encuentran en la sección 6.3 de la Política de Certificación de la ACRN [3].

6.3.2. Protección de la clave privada de la Persona Jurídica

Únicamente el Suscriptor del certificado puede utilizar la clave privada correspondiente.

La protección de la clave privada del certificado de Persona Jurídica no puede ser delegada y es responsabilidad exclusiva del Suscriptor. No se permite la realización de respaldos de la clave privada ni acuerdos de *escrow*.

La clave privada, cuando no esté siendo utilizada, debe encontrarse desactivada. Para activar la clave para su uso se debe proveer un PIN.

Este PIN debe tener un largo mínimo de 8 caracteres alfanuméricos. El Suscriptor debe proteger el PIN de forma que quede bajo su exclusivo control.

Cuando la persona jurídica deje de utilizar la clave privada, debe desactivarla inmediatamente. La desactivación fuerza a ingresar el PIN nuevamente para utilizarla.

Al finalizar el período de validez del certificado, en caso de que no sea posible o no se desee su renovación, se recomienda al suscriptor la destrucción de la clave privada.

6.4. Otros aspectos de la gestión del par de claves

El período de validez máximo del certificado es de dos años, pudiendo ser renovado un máximo de dos veces. En cualquier caso, es responsabilidad del PSCA que ningún certificado tenga una validez superior a dos años, y que el fin de la validez de ninguno de ellos sea posterior a los 6 años desde que se generó el par de claves en la emisión original. Ver sección 4.6.

6.5. Datos de activación

La clave privada de persona jurídica debe ser protegida mediante un PIN conforme se indica en la sección 6.3 de la presente Política de Certificación.

El PSCA debe proteger la clave privada de la ACPA conforme se especifica en la sección 6.3 de la Política de Certificación de la ACRN [3].

6.6. Controles de seguridad informática

Los controles de seguridad informáticos que los PSCA deben implementar se encuentran especificados en la sección 6.6 de la Política de Certificación de la ACRN [3].

La persona jurídica debe tener controles de acceso que garanticen la protección de los sistemas que hacen uso de la clave privada de firmado.

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

Los controles de seguridad sobre el ciclo de vida de los sistemas que los PSCA deben implementar se encuentran especificados en la sección 6.7 de la Política de Certificación de la ACRN [3].

6.8. Seguridad de la red

Los controles de seguridad de la red que los PSCA deben implementar se encuentran especificados en la sección 6.8 de la Política de Certificación de la ACRN [3].

6.9. Sincronización horaria

Los controles de sincronización horaria que los PSCA deben implementar se encuentran especificados en la sección 6.9 de la Política de Certificación de la ACRN [3].

7. Perfiles de Certificado y CRL

El formato de los certificados de Persona Jurídica deben cumplir con lo especificado en el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), mientras que la lista de revocación de certificados debe cumplir con el mismo estándar, pero en su versión 2. Ambos están definidos en su versión más reciente en el RFC 5280 [6].

Adicionalmente, para los perfiles que contemplen curvas elípticas deberán ser con el estándar respectivo:

Curvas NIST (RFC 6979)

Curvas Brainpool (RFC 5639)

Curvas Edwards (RFC 8032)

En todos los casos, la codificación de caracteres de los certificados, listas de revocación y mensajes OSCP si correspondiere, debe ser UTF-8.

7.1. Perfil de certificado de Persona Jurídica

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

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACPA emisora
Algoritmo de Firma (Signature Algorithm)	sha256RSA sha384RSA ECC-Brainpool (conforme RFC 5639) Curve25519 (Conforme RFC 7748) Ed25519 (PureEdDSA y HashEdDSA RFC 8032) sha256WithECDSAEncryption
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA emisora tal cual figura en su certificado
Validez (Valid From / Valid To)	0 a 2 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor	CN = Nombre de Fantasía de la Organización

(Subscriber DN)	<p>O = Nombre legal de la Organización</p> <p>C = UY</p> <p>serialNumber = Tipo y número de registro</p> <p>(Ver sección 3.1.1)</p>
Clave Pública del Suscriptor (Subject Public Key)	<p>Clave pública RSA de 2048 bits o más</p> <p>brainpoolP256r1</p> <p>Curve25519 (256 bits)</p> <p>Ed25519 (256 bits)</p> <p>Nistp-256 (256 bits)</p> <p>Nistp-384 (384 bits)</p>
Extensiones	
Identificador de la clave del	Hash de 20 bytes del atributo Subject Public Key

suscriptor (Subject Key Identifier)	
Identificador de la clave de la autoridad (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la ACPA emisora
Uso de Claves (Key Usage)	<p>DigitalSignature = 1</p> <p>NonRepudiation/contentCommitment = 1</p> <p>KeyEncipherment = 1</p> <p>DataEncipherment = 1</p> <p>KeyAgreement = 0</p> <p>KeyCertSign = 0</p> <p>CRLSign = 0</p> <p>EncipherOnly = 0</p> <p>DecipherOnly = 0</p>
Uso de Claves Extendido (Extended Key Usage)	clientAuth
Políticas de Certificación (Certificate Policies)	<p>OID: 2.16.858.10000157.66565.4</p> <p>URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/cp_personajuridica_v2.0.pdf</p> <p>OID: OID asignado a la CPS del PSCA para la ACPA emisora</p> <p>URI: URL de publicación de la CPS</p>
Restricciones Básicas (Basic Constraints)	CA = FALSE

Puntos de distribución de las CRL (CRL Distribution Points) URI = URL primaria de publicación de la CRL
URI = URL secundaria de publicación de la CRL

7.2. Perfil de la CRL de las ACPA de PSCA

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

Atributos	Contenido
Versión (Version)	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA sha384RSA sha512RSA Nistp521 (521 bits) BrainpoolP512r1 (512 bits) Ed448 (448 bits)
Nombre Distintivo del Emisor (Issuer)	DN de la ACPA tal cual figura en su certificado
DN)	
Día y Hora de Emisión (Effective 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 ACPA
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

8. Administración Documental

8.1. Procedimiento para cambio de especificaciones

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

En caso de que un PSCA desee una modificación en la presente política deberá realizar la solicitud a la UCE con la correspondiente justificación, la UCE evaluará la solicitud y en caso de aprobarla, realizará la modificación y posterior publicación de la nueva versión.

La CPS de las ACPA será generada por el PSCA y aprobada por la UCE, para cambiarla se deberá solicitar autorización a la UCE.

8.2. Procedimientos de Publicación y Notificación

La UCE publicará en su sitio web las modificaciones aprobadas a la presente Política de Certificación, indicando en cada caso las secciones y/o textos remplazados junto con la publicación de la nueva versión.

Además, publicará un vínculo a los mismos en el Diario Oficial durante un (1) día hábil.

Lo anteriormente estipulado también aplica a las Condiciones para la Utilización de Firma Electrónica Avanzada [4]. Los PSCA deberán notificar a sus suscriptores de cualquier cambio en estas condiciones o en la presente Política de Certificación.

De la misma forma, los PSCA deberán publicar en su sitio web cualquier modificación que realicen en sus Prácticas de Certificación que deberán ser aprobadas por la UCE y notificar a los usuarios finales de los cambios realizados en caso de ser necesario.

Referencias Externas

1: Chokhani, Ford, Sabett, Wu, RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 2003

2: Poder Legislativo, República Oriental del Uruguay, Ley N° 18.600 de Documento y Firma Electrónicos, 21 de setiembre de 2009

3: Unidad de Certificación Electrónica, Política de Certificación de la Autoridad Certificadora Raíz Nacional, aprobada por Resolución N° 2/011, de 5 de octubre de 2011

4: Unidad de Certificación Electrónica, Condiciones para la Utilización de Firma Electrónica Avanzada, 2012

5: Poder Ejecutivo, República Oriental del Uruguay, Decreto N° 436/011, Reglamentación de la Ley de Firma y Documento Electrónicos, 8 de diciembre de 2011

6: Cooper, Santesson, Farrell, Boeyen, Housley, Polk, RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008