Política de Certificación de Servidor SSL/TLS

Unidad de Certificación Electrónica

Infraestructura Nacional de Certificación Electrónica
República Oriental del Uruguay

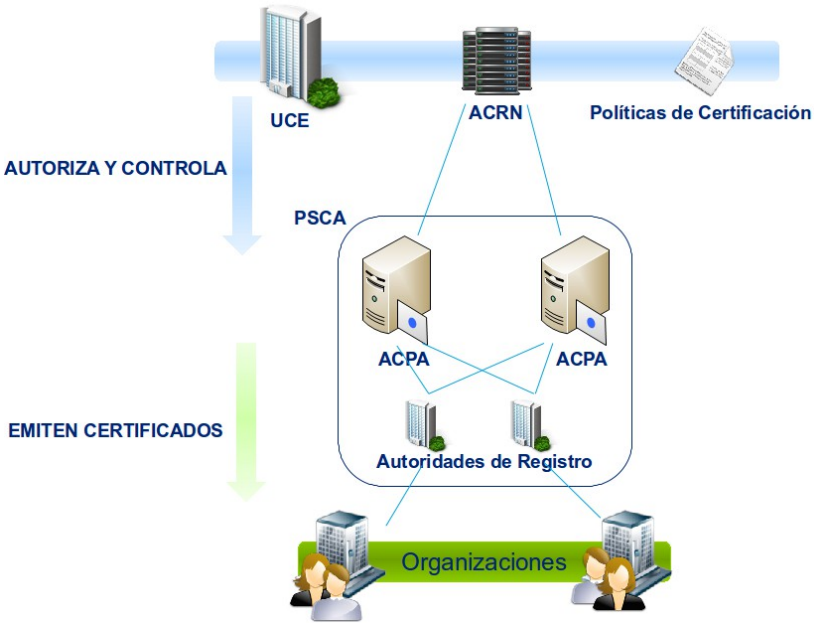
Índice

1.Introducción

1.1.Descripción general

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 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.

Un Certificado Electrónico de Servidor SSL/TLS 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), con el fin de asegurar comunicaciones.

La presente Política de Certificación de Servidor SSL/TLS rige la actividad de los PSCA cumpliendo los requerimientos de “Certification Authority / Browser Forum Baseline Requirements (CABF Baseline Requirements)” [1] de manera de emitir certificados públicamente confiables. El CABF Baseline Requirements está publicado en https://www.cabforum.org. Si existe alguna inconsistencia entre esta política de certificación y los Baseline Requirements, los Baseline Requirements tienen prioridad. 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 Servidor SSL/TLS.

La confección del presente documento se realizó siguiendo el marco normativo vigente y los lineamientos 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 [2]. Para preservar el esquema especificado en RFC 3647, las secciones que no aplican tienen la declaración "No es aplicable" o "No estipulado".

1.2.Nombre del documento e Identificación de la Política de Certificación

Nombre: Política de Certificación de Servidor SSL/TLS

Versión: 1.0

Fecha de elaboración: 19/09/2014

Fecha de última actualización: 19/09/2014

OID: 2.16.858.10000157.66565.9

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

1.3.Participantes de la INCE

1.3.1.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 [3], 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 [4] y en el artículo 14 de la Ley N° 18.600, de 21 de Setiembre del 2009 [3].

1.3.2.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 [4]. 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 emitir certificados a otra ACPA para que actúe como su subordinada.

De acuerdo con lo estipulado en la Política de Certificación de la ACRN [4], 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.

1.3.3.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 1.3.4). 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 o jurídica 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.

Las responsabilidades y acciones realizadas por la Autoridad de Registro se encuentran descriptas en la sección 9.17.3.4 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.

1.3.4.Suscriptores

En el contexto de la presente Política de Certificación, los Suscriptores hace referencia a una persona, una organización o una entidad que es el sujeto de un Certificado, o propietario del dispositivo que es el sujeto del Certificado y para la que se ha emitido dicho Certificado, y puede utilizar y está autorizada a utilizar la clave privada asociada a la clave pública recogida en el Certificado de prueba en cuestión.

En la presente política se validan dominios y/o direcciones IP, por lo tanto los suscriptores podrán ser los propietarios del dominio o dirección IP o que posean control sobre los mismos, teniendo la autoridad final sobre la clave privada correspondiente a la clave pública que aparece en el Certificado del suscriptor.

Los Suscriptores contraen derechos y obligaciones al utilizar certificados de Servidor SSL/TLS según se describe en la presente Política de Certificación y normativa vigente.

1.3.5.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 realización de comunicaciones seguras utilizando el protocolo SSL o TLS.

Los Terceros Aceptantes, al utilizar el certificado para una conexión segura, están obligados a comprobar la validez del certificado. Para ello, deberán seguir los lineamientos estipulados en esta Política.

1.3.6.Otros participantes

No es aplicable.

1.4.Uso de los certificados

1.4.1.Usos Permitidos de los Certificados

Los usos habilitados para los certificados emitidos bajo la presente Política de Servidor SSL/TLS son los estipulados en los campos “key usage” y “extended key usage” que se encuentran en el certificado.

Esto implica que se utilizarán para asegurar las comunicaciones mediante el protocolo SSL o TLS el cual podrá proveer:

- Autenticación
- Aseguramiento acerca de la identidad de un dispositivo remoto
- Encriptación

1.4.2.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 1.4.1, y a la normativa vigente.

Los certificados no garantizan que el sujeto sea de confianza, que opere una empresa de buena reputación ni que el equipamiento donde se instalo el certificado este libre de defecto o malware.

1.5.Administración de la Política de Certificación

1.5.1.Organización administradora del documento

La administración de la presente Política de Certificación de Servidor SSL/TLS es responsabilidad de la UCE.

1.5.2. Persona de Contacto

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 2929

1.5.3. Persona que determina la idoneidad de la CPS

La actividad de los PSCA se encuentra regulada por la Unidad de Certificación Electrónica (UCE) y sujeta a sus procedimientos de control. Cada PSCA presenta a la UCE un documento denominado Declaración de Prácticas de Certificación (CPS) en el cual declara los procedimientos administrativos y técnicos mediante los cuales satisface lo exigido por la Política de Certificación. La UCE valida que la Declaración de Prácticas de Certificación cumpla con lo estipulado en la presente política de manera que el Prestador pueda emitir certificados bajo la misma.

1.5.4. Procedimiento de aprobación de la CPS

No estipulado.

1.6.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 [3] 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.

1.7.Procedimiento de Aprobación de la presente política

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.

1.8.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 [3]. No obstante, las siguientes definiciones y abreviaturas son utilizadas a lo largo del presente documento, y por lo tanto, son citadas también aquí.

Solicitante: La persona física o jurídica que solicita (o busca renovar) un Certificado. Una vez que el certificado es emitido, la persona se conoce como el Suscriptor. Para los certificados emitidos a dispositivos, el solicitante es la persona que controla u opera el dispositivo nombrado en el certificado, incluso si el dispositivo es el que manda el CSR.

Representante del solicitante: La persona física que es el solicitante o bien un agente autorizado que tiene autorización expresa para representar a el solicitante:

1. Quien firma y presenta o aprueba un pedido de certificado en nombre del solicitante, y/o
2. Quien firma y presenta un acuerdo de suscriptor en nombre del solicitante

Suscriptor: Persona física o jurídica a quien es emitido el certificado y quien es legalmente sometido a un acuerdo de suscriptor. Ver 1.3.4.

Tercero aceptante: Ver 1.3.5.

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 (RA – Registration Authority): 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. Ver 1.3.3.

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.

Acuerdo de suscriptor: un acuerdo entre un ACPA y el solicitante/suscriptor que especifica los derechos y responsabilidades de las partes.

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.

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.

Custodia de clave (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:

1. Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;

2. 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,

3. 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.

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.

Dirección IP reservada : Una dirección IPv4 o IPv6 que el IANA marco como reservado:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Nombre Interno: Cadena de caracteres (no una dirección IP) en un campo Common Name o Subject Alternative Name de un certificado que no puede ser verificado como globalmente único en el DNS público al momento de emisión del certificado porque no termina con un Top Level Domain (TLD) registrado en la base de datos de zonas raíz de la IANA.

Nombre de dominio registrado: Un nombre de dominio que ha sido registrado con un Registrador de nombre de dominio.

Registrador de nombre de dominio: Una persona o entidad que registra nombres de dominio bajo el auspicio de: (i) la 'Internet corporation for Assigned Names and Numbers' (ICANN), (ii) una autoridad/registrador nacional de nombre de dominio, o (iii) un Centro de información de red (incluyendo sus filiales, contratistas, delegados, sucesores o cesionarios).

Nombre de dominio completamente calificado (FQDN – Fully Qualified Domain Name): Un nombre de dominio que contiene todas las etiquetas de los nodos superiores en el sistema de nombres de dominio de internet.

Titular del nombre de dominio registrado: Persona o entidad que registra un nombre de dominio ante un Registrador de nombre de dominio y que tiene el derecho de controlar como es usado tal nombre de dominio, así como la Persona Natural o Jurídica que es presentada por el registrador mediante el sistema WHOIS.

Certificado comodín (Wildcard Certificate): Certificado que contiene un asterisco (*) a la izquierda del FQDN contenido en el sujeto del certificado, indicando que soporta cualquier prefijo unitario del mismo.

Protocolo de desafío-respuesta: Los protocolos desafío-respuesta permiten la autenticación de entidades mediante el siguiente sistema:

- Una parte (verificador) presenta una pregunta (desafío).
- La parte que se quiere autenticar recibe la pregunta y elabora una respuesta que envía al verificador.

- El verificador recibe la respuesta y evalúa si la respuesta es correcta para la pregunta, y por tanto la entidad que envió la respuesta queda autenticada, o no.

NIST (National Insitute of Standars 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.

2.Responsabilidades de publicación y repositorio

2.1.Repositorios

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.

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 [4].

La UCE utilizará como repositorio para las distintas políticas aprobados incluyendo la presente política el siguiente sitio web:

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

Además, en el contexto de la presente Política publicará la siguiente información adicional:

1. Esta Política de Certificación (versión vigente y anteriores);
2. La lista de OIDs de la Declaración de Prácticas de Certificación de los PSCA que emiten certificados de Servidor SSL/TLS;
3. Información relevante de los informes de auditoría de la que fueron objeto los PSCA que emiten certificados de Servidor SSL/TLS;

4. Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos designados por los PSCA que emiten certificados de Servidor SSL/TLS, 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 [4]. Además, en el contexto de la presente Política deberá publicar la siguiente información adicional:

1. Esta Política de Certificación (versión vigente y anteriores);

2. Los certificados emitidos para ACPA que emitan certificados de Servidor SSL/TLS.

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

1. Todas las políticas de certificación (versiones vigentes y anteriores) que utilicen las ACPA del PSCA para la emisión de certificados, incluyendo ésta;

2. La Declaración de Prácticas de Certificación de cada una de las ACPA del PSCA (versión vigente y anteriores);

3. El Acuerdo con la ACRN que lo oficializa como suscriptor de Certificados de la ACRN;

4. El certificado emitido por la ACRN para cada una de sus ACPA;

5. La Lista de Certificados Revocados (CRL) de la ACPA;

6. 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;

7. Referencia al sitio de publicación de información de la UCE;

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.

2.2.Publicación de la Información de certificación

La UCE publicará en su sitio web las modificaciones aprobadas a la presente Política de Certificación, indicando en cada. Además, publicará un vínculo a los mismos en el Diario Oficial durante un (1) día hábil.

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, así como cualquier cambio en el acuerdo del suscriptor.

2.3.Tiempo o frecuencia de la Publicación

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

2.4.Controles de Acceso a los Repositorios

La UCE brinda acceso irrestricto a toda la información contenida en el repositorio público (ver 2.1), 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) y establecer los controles necesarios para restringir la escritura o modificación de la información publicada.

2.5.Servicio de Validación de Certificados

Los PSCA deberán mantener páginas web que permitan a los proveedores de software de aplicación probar su software con certificados de suscriptor SSL/TLS que se encadenan a el certificado de la ACRN. Como mínimo el PSCA deberá proveer de paginas web separadas para certificados de Servidor SSL/TLS (i) valido, (ii) revocado, y (iii) expirado.

3.Identificación y Autenticación

En los Certificados de Servidor SSL/TLS emitidos bajo la presente política se harán una de dos tipos de validación – Validación de Dominio (DV) y Validación Organizacional (OV) dando como resultado Certificados de Dominio Validado y Certificados de Organización Validada respectivamente.

En los certificados de tipo DV, mínimamente se validarán un conjunto de dominios o direcciones IP para las cuales se emitirá el certificado. En los certificados de tipo OV, se podrá identificar y autenticar adicionalmente un individuo u organización asociado a los dominios y/o IP validadas. De esta manera se cumplen los requerimientos CABF Baseline Requirements [1].

3.1.Nombres

3.1.1.Tipos de Nombres

Los certificados emitidos bajo la presente política contendrán un nombre X.501 Distinguished Name (DN) tanto pata el sujeto como para el emisor.

El campo del emisor contendrá el DN de la ACPA emisora tal cual figura en su certificado.

Los nombres de dominios o direcciones IP verificadas serán ubicadas obligatoriamente en la extensión del certificado Subject Alternative Name, siendo completada con por lo menos un nombre de dominio o dirección IP usando el tipo de atributo correspondiente, y opcionalmente en el campo CN del Distinguished Name. Los nombres de dominio serán FQDN y se permite el uso de Wildcard FQDN.

No está permitido el uso de direcciones IP Reservadas o Nombres Internos.

3.1.1.1.Tipos de nombre de sujeto para certificados DV

El atributo Subject Distinguished Name del certificado de Dominio Validado deberá contener obligatoriamente un campo de tipo OU indicando que el certificado es de Dominio Validado de la siguiente forma:

Organizational Unit Name (OU – OID 2.5.4.11) = Control de Dominio Validado.

El campo Country (C – OID 2.5.4.6) será obligatorio, y el código del país deberá ingresarse según la nomenclatura ISO 3166-1 (por ejemplo: UY para Uruguay).

El campo Common Name (CN – OID 2.5.4.3) podrá ser utilizado para indicar el nombre de dominio o dirección IP principal que se está certificando cuando sea necesario por motivos de compatibilidad.

3.1.1.2. Tipos de nombre de sujeto para certificados OV

La información del sujeto a completar en el atributo Subject Distinguished Name del certificado de Organización Validada será de la siguiente forma:

Organization Name (O – OID 2.5.4.10): Nombre de la organización o nombre del individuo según fue verificado acorde a 3.2. Si la validación es de un individuo se colocara el nombre del individuo en el campo O según es indicado en los CABF Baseline Requirements [1].

Street Address (STREET – OID 2.5.4.9): Opcionalmente se podrá incluir aquí la dirección de las oficinas principales de la organización o el individuo luego de que haya sido verificada la información acorde a 3.2.

Locality Name (L – OID 2.5.4.7): Ciudad donde se encuentran las oficinas principales de la organización. Obligatorio.

Estado o provincia (ST – OID 2.5.4.8): Departamento/Estado/Provincia donde se encuentran las oficinas principales de la organización. Obligatorio.

Postal Code (OID – 2.5.4.17): Código postal. Opcional.

Country Name (C – OID 2.5.4.6): Código del país según la nomenclatura ISO 3166-1 (UY). Obligatorio.

Organizational Unit Name (OU – OID 2.5.4.11) = Organización Validada. Obligatorio.

El campo Common Name (CN – OID 2.5.4.3) podrá ser utilizado para indicar el nombre de dominio o dirección IP principal que se está certificando cuando sea necesario por motivos de compatibilidad.

3.1.2. Necesidad de que los nombres sean significativos

No estipulado.

3.1.3.Anonimato o Seudónimos de los Suscriptores

En el caso de los Certificados DV, alcanzará con que se valide posesión del dominio, siendo el suscriptor anónimo. En cuanto a los certificados OV no se permite el anonimato, por lo que se debe validar el individuo o la organización suscriptora como es estipulado en 3.2.

3.1.4.Reglas de interpretación de diversas formas de nombre

Los nombres distinguidos en los certificados son interpretados usando estándares X.500 y sintaxis ASN.1. Ver RFC 4514 [6] y RFC 2616 [7] para mayor información en como los nombres distinguidos X.500 en los certificados son interpretados como URIs (Uniform Resources Identifiers) y referencias http.

3.1.5.Unicidad de los nombres

Las ACPA deben forzar la unicidad de los nombres en los certificados emitidos bajo la Infraestructura Nacional de Certificación Electrónica.

3.1.6.Reconocimiento, autenticación, y el rol de las marcas comerciales

Los suscriptores no deberán solicitar certificados con algún contenido que infrinja los derechos de propiedad intelectual de otra entidad. Sin embargo, esta CP no requiere que se verifique el derecho de un solicitante a utilizar una marca comercial, por lo que los PSCA no serán responsables por la verificación de este punto.

3.2.Validación de Identidad Inicial

La Autoridad de Registro del PSCA deberá realizar la identificación del solicitante de un certificado usando cualquier medio legal de comunicación o investigación necesaria para identificar una persona jurídica o física.

3.2.1.Método para probar la posesión de la clave privada

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. En el caso de certificados DV, alcanza con registrar una dirección de correo electrónico del referente, mientras que para certificados OV se debe registrar además el nombre completo y documento de identidad del referente.

3.2.2.Autenticación de la identidad de una organización

Para los Certificados de tipo OV, se requiere que los solicitantes indiquen el nombre de la organización y su dirección.

La validación de la identidad de la organización, del individuo y su correspondiente representación se deben realizar de igual manera que en la Política de Certificación de Persona Jurídica, capítulo 3.1.2.

3.2.3.Autenticación de la identidad de un individuo

En el caso de los Certificados OV solicitados por un individuo se deberá verificar que toda información provista en el nombre del sujeto corresponda al Solicitante del Certificado, para lo cual se debe realizar la misma validación de identidad que en la Política de Certificación de Persona Física, capítulo 3.1.2.

3.2.4.Autenticación del dominio

Las ACPA deberán asegurar que, a la fecha en que el Certificado fue emitido, el Solicitante, su casa matriz o una subsidiaria directa, cumple con alguno de los siguientes puntos:

- Tenía derecho a usar, o tenía el control del FQDN; o
- Fue autorizado por una persona que tenía derecho o control del FQDN que figuran en el Certificado.

Para demostrar control sobre un dominio se podrá requerir que el solicitante cargue información generada aleatoriamente (clave única) específica a una página definida o registro DNS del dominio, la cual será consultada por la ACPA para verificar que el solicitante efectivamente tiene control sobre el mismo. De verificarse esta información, se da por validado el control del dominio.

Si la ACPA utiliza un mecanismo de desafío-respuesta para confirmar que el Solicitante cuenta con autorización del Titular del nombre de dominio, la CA deberá utilizar una dirección de correo electrónico para tal mecanismo formado de una de las siguientes maneras:

1. Suministrado por el Registrador de nombre de dominio;

2. Tomado del campo "registrant", "technical contact" o "administrative contact" de la información de contacto del Titular del nombre de dominio que aparece en el registro WHOIS del Dominio, o;

3. Usando como nombre de usuario alguna de las siguientes: 'admin', 'administrator', 'administrador', 'webmaster' o 'hostmaster', y el Nombre de Dominio Formado quitando cero o más componentes del Nombre de Dominio Registrado o del FQDN solicitado.

Si el Titular del nombre de dominio ha utilizado un servicio de registro privado, anónimo, o delegado, y la CA se basa en una Autorización de Dominio como una alternativa a lo anterior, la Autorización de Dominio debe ser recibida directamente desde el servicio de registro privado, anónimo, o delegado identificado en el registro WHOIS del Nombre de Dominio Registrado. El documento debe contener:

- El membrete del servicio de registro privado, anónimo, o delegado;

- La firma del Gerente General, o su equivalente, o un representante autorizado de dicho funcionario, fechada en o después de la fecha de solicitud de certificado.

- El (los) nombre(s) de dominio(s) autorizados

Si el registro WHOIS identifica el servicio de registro privado, anónimo o delegado, como el Titular del Nombre de Dominio, entonces la autorización de dominio deberá contener una declaración que concede al Solicitante el derecho a utilizar el FQDN en un Certificado. La ACPA se pondrá en contacto directamente con el servicio de registro privado, anónimo o delegado, usando la información de contacto obtenida de una fuente

de tercera parte confiable e independiente y obtendrá la confirmación del Titular del Nombre de Dominio de que la Autorización de Dominio es auténtica.

Antes de emitir un certificado wildcard, la ACPA debe establecer y seguir un procedimiento documentado que determine si el carácter wildcard (*) ocurre en la primera posición a la izquierda de un dominio controlado por un Registrar o es sufijo publico (por ejemplo *.com, *.com.uy, *.uy, *.co.uk, etc. ver RFC 6454 sección 8.2).

En caso que el wildcard se ubique en la primera posición a la izquierda de un dominio controlado por un Registrar o sufijo público, la ACPA deberá rechazar la emisión. Por ejemplo, la ACPA no podrá emitir *.com.uy ni *.uy, pero podrá emitir *.ejemplo.com.uy o *.ejemplo.uy a “Compañía Ejemplo".

La determinación de que es controlado por un Registrar o es un sufijo público no está estandarizada al momento de escribir la presente política y no es una propiedad del DNS por sí mismo. En el contexto de la INCE, la práctica que deberán seguir los PSCA será consultar la lista de sufijos públicos en https://publicsuffix.org/list/effective_tld_names.dat (PSL – Public Suffix List), y mantener una copia actualizada regularmente, considerando únicamente como restringidos los dominios ICANN, no los dominios privados.

3.2.5.Autenticación de las direcciones IP

Las ACPA deberán asegurar que, a la fecha en que el Certificado fue emitido, el Solicitante tenía derecho a usar, o tenía el control de las direcciones IP que figuran en el Certificado mediante:

- Demostración de que el solicitante tiene control practico sobre la dirección IP haciendo un cambio acordado a la información encontrada en una página web identificada por una URI que contiene a la dirección IP;
- Obteniendo documentación acerca de la asignación de la dirección IP a través de LACNIC;
- Usando cualquier otro método de confirmación, de manera que el ACPA mantenga evidencia documentada que el solicitante tiene control sobre la dirección IP de por lo menos el mismo nivel de aseguramiento que los puntos anteriormente mencionados.

3.2.6.Información no verificada del suscriptor

Los Certificados emitidos bajo la presente política no podrán contener información del suscriptor no verificada.

3.2.7.Validación de la autoridad

No es aplicable

3.2.8.Criterios para la interoperación

No es aplicable.

3.3.Identificación y Autenticación para las solicitudes de reasignación de claves

El procedimiento de cambio de clave es el de Emisión de Certificado, por lo que se aplica lo mismo que para el punto 3.2.

3.3.1.Identificación y autenticación para la reasignación de clave rutinaria

El procedimiento de cambio de clave es el de Emisión de Certificado, por lo que se aplica lo mismo que para el punto 3.2.

3.3.2.Identificación y autenticación para la reasignación de clave luego de la revocación

El procedimiento de cambio de clave es el de Emisión de Certificado, por lo que se aplica lo mismo que para el punto 3.2.

3.4.Identificación y Autenticación para la Solicitud de Revocación

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 4.9.1.

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 3.2).

Para la solicitud remota, el referente del certificado es la persona autorizada a solicitar la revocación, por lo que el ACPA deberá autenticarlo apropiadamente, por ejemplo mediante un desafío-respuesta al correo electrónico o teléfono que tiene registrado desde el registro.

El PSCA contará con 24 horas para verificar la documentación y autenticar la solicitud, y entonces la revocación deberá realizarse en forma inmediata. 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.

4.Requerimientos operativos del ciclo de vida de los certificados

4.1.Solicitud de certificados

4.1.1.Quién puede presentar una solicitud de certificado

Para la solicitud del certificado de tipo OV, 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.

Para la solicitud del certificado DV podrá actuar cualquier persona en forma anónima, ya que la validación es sólo del dominio y no del individuo u organización que lo opera.

4.1.2.Proceso de enrolamiento y responsabilidades

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.

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 6.1.1. 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 el acuerdo del suscriptor.

4.2.Procesamiento de solicitud de certificado

4.2.1.Realización de funciones de identificación y autenticación

Las ACPA deberán mantener los sistemas y procesos para autenticar satisfactoriamente a los solicitantes en linea con las declaraciones hechas en su CPS. La validación de identidad inicial se podrá realizar por un equipo de validación de la ACPA o un tercero bajo contrato en linea con la sección 3.2 de esta política.

4.2.2.Aprobación o rechazo de las solicitudes de certificado

Una vez que la Autoridad de Registro del PSCA registró la solicitud de certificado – según se especifica en la sección 4.1.2 - 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.

4.2.3.Plazo para procesar las solicitudes de certificado

El plazo entre el registro de solicitud de un certificado (dado por la validación 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 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 39 meses. 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 suscriptora si corresponde.

4.3.1.Acciones de la CA durante la emisión del certificado

Las ACPAs deberán usar las cuentas capaces de emitir certificados de sus Autoridades de Registro mediante autenticación multifactor. Las RA directamente operadas por la ACPA emisora o los terceros contratados por la ACPA para realizar las validaciones deberán asegurar que toda la información enviada a la ACPA sea verificada y autenticada de manera segura.

4.3.2.Notificaciones al suscriptor de la emisión del certificado por parte de la CA

La ACPA emisora deberá informar al suscriptor de la emisión de el Certificado de una manera conveniente y apropiada basado en la información suministrada en el proceso de enrolamiento.

4.4.Aceptación del certificado

4.4.1.Conducta que constituye aceptación del certificado

La ACPA emisora deberá informar a los suscriptores que no deberán usar el Certificado hasta no haber revisado y verificado la precisión de los datos incluidos en el mismo. La ACPA emisora podrá establecer un limite de tiempo luego del cual el certificado se considerará aceptado.

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 4.9.5 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.

4.4.2.Publicación del certificado por la CA

La ACPA emisora podrá publicar el Certificado enviando el Certificado a el suscriptor y/o publicando el mismo en un repositorio adecuado.

4.4.3.Notificación de la emisión del certificado a otras entidades por parte de la CA

No estipulado.

4.5.Uso del par de claves y del certificado

4.5.1.Uso de la clave privada y certificado por el suscriptor

El Suscriptor puede utilizar el certificado y su par de claves únicamente para los fines descriptos en la sección 1.4 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 el acuerdo del Suscriptor .

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

En caso que el Suscriptor sospeche del compromiso de la clave privada, debe solicitar la revocación inmediata del certificado al PSCA. (Ver 4.9.1).

4.5.2.Uso de la clave pública y certificado por el tercero aceptante

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

- El certificado es válido y fue emitido por un PSCA de la INCE;
- El certificado se está utilizando para uno de los usos permitidos en esta Política de Certificación (ver 1.4);
- 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;
- El certificado del PSCA emisor es válido de acuerdo con la Política de Certificación de la ACRN, y
- El certificado de la ACRN es válido.

4.6.Renovación de certificado

La renovación de un certificado consiste en la emisión de un nuevo certificado con la misma información que el anterior incluyendo la clave pública a excepción del periodo de validez.

4.6.1.Circunstancias para la renovación de certificado

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.

La validez de los certificados deberá ser, como máximo, de 39 meses, y la cantidad de renovaciones no está restringida, siempre y cuando el par de llaves no tenga una duración superior a 78 meses (una emisión por tiempo máximo y una renovación análoga).

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.

4.6.2.Quién puede solicitar la renovación

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.

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

4.6.3.Procesamiento de solicitudes de renovación de certificado

La ACPA emisora podrá requerir información adicional antes de procesar la solicitud de renovación.

4.6.4.Notificación al suscriptor de la emisión de un nuevo certificado

Se realizará de la misma manera a como está estipulado en el punto 4.3.2 .

4.6.5.Conducta que constituye aceptación del certificado de renovación

Se realizará de la misma manera a como está estipulado en el punto 4.4.1 .

4.6.6.Publicación del certificado renovado por la CA

Se realizará de la misma manera a como está estipulado en el punto 4.4.2

4.6.7.Notificación de la emisión del certificado por parte de la CA a otras entidades

Se realizará de la misma manera a como está estipulado en el punto 4.4.3

4.7.Reasignación de claves del certificado

La reasignación de claves de un certificado consiste en la emisión de un nuevo certificado con la misma información que el anterior pero con distinta clave pública y periodo de validez.

4.7.1.Circunstancias para la reasignación de claves del certificado

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 reasignación de claves no es un procedimiento válido.

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

En el caso de la reasignación de claves, 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.

4.7.2.Quién puede solicitar la certificación de una nueva clave pública

El Solicitante debe autenticar su solicitud de reasignación de claves de forma idéntica a la solicitud original, conforme lo requiere el punto 4.1 de esta Política.

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

4.7.3.Procesamiento de solicitudes de reasignación de claves del certificado

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

4.7.4.Notificación al suscriptor de la emisión de un nuevo certificado

Se realizará de la misma manera a como está estipulado en el punto 4.3.2 .

4.7.5.Conducta que constituye aceptación del certificado para claves reasignadas

Se realizará de la misma manera a como está estipulado en el punto 4.4.1 .

4.7.6.Publicación del certificado de clave reasignada por la CA

Se realizará de la misma manera a como está estipulado en el punto 4.4.2

4.7.7.Notificación de la emisión del certificado por parte de la CA a otras entidades

Se realizará de la misma manera a como está estipulado en el punto 4.4.3

4.8.Modificación del certificado

4.8.1.Circunstancias para la modificación del certificado

La modificación de un certificado es definida como la creación de un nuevo certificado que contiene la información modificada respecto a un certificado previamente emitido.

El nuevo certificado modificado podrá o no tener una nueva clave pública y podrá o no tener una nueva fecha de vencimiento.

La ACPA emisora deberá tratar una modificación de un certificado como una nueva emisión.

La ACPA emisora podrá modificar certificados que fueron previamente renovados o se le reasignaron las claves previamente. El certificado original podrá ser revocado luego que la modificación fuera completada, sin embargo, el certificado original no podrá ser renovado, ni se le podrá aplicar una reasignación de claves ni modificarlo .

4.8.2.Quién puede solicitar modificación del certificado

Idem 4.1

4.8.3.Procesamiento de solicitudes de modificación del certificado

Idem 4.2

4.8.4.Notificación al suscriptor de la emisión de un nuevo certificado

Idem 4.3.2

4.8.5.Conducta que constituye aceptación del certificado modificado

Idem 4.4.1

4.8.6.Publicación del certificado modificado por la CA

Idem 4.4.2

4.8.7.Notificación de la emisión del certificado por parte de la CA a otras entidades

Idem 4.4.3

4.9.Revocación y suspensión de certificado

4.9.1.Circunstancias para la revocación

La suspensión de un certificado no es una operación permitida.

Las causas de revocación de un certificado son las siguientes:

- solicitud de representante legal de la organización identificada en el certificado;
- pérdida, sospecha de compromiso o destrucción del soporte donde se encuentra almacenada la clave privada del certificado;
- pérdida, sospecha de compromiso o destrucción de la clave privada del certificado;
- datos erróneos o inexactos en el certificado;
- disolución de la organización identificada en el certificado;
- revocación de la ACPA del PSCA que emitió el Certificado;
- resolución judicial que así lo determine;
- 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.

4.9.2.Quién puede 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 4.9.1, los siguientes actores:

- un representante legal de la organización identificada en el certificado,
- el individuo representado en el certificado,
- todo individuo registrado como titular de algún dominio identificado como sujeto del certificado,
- el solicitante original, contactado por algún método por los cuales se registró,
- el mismo PSCA; y,
- la UCE.

4.9.3.Procedimiento para la solicitud de revocación

Una vía para la solicitud de revocación de un certificado es 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. 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 Servidor SSL/TLS. El PSCA deberá realizar las mismas verificaciones de identidad de la persona física y las facultades que tiene para solicitar la revocación, de forma análoga a cómo se realiza en el caso de la emisión de certificado (Ver sección 4.2.1).

Otra vía es la solicitud remota. En esta vía, el referente del certificado es la persona autorizada a solicitar la revocación, por lo que el ACPA deberá autenticarlo apropiadamente, por ejemplo mediante un desafío-respuesta al correo electrónico o teléfono que tiene registrado desde el registro.

Ambas vías son de implementación obligatoria para el PSCA.

En cualquier situación de revocación, el PSCA deberá confirmar al Suscriptor la revocación una vez sea efectiva la misma.

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.

4.9.4.Periodo de gracia de solicitud de revocación

No estipulado.

4.9.5.Tiempo dentro del cual la CA debe procesar la solicitud de revocación

El PSCA contará con un máximo de 24 horas para la validación de la solicitud de revocación y su documentación asociada, momento en el cual deberá autenticarla o declararla no válida especificando las causas.

Luego de la autenticación de la solicitud, el PSCA contará con un plazo máximo de 2 horas para efectivizar la revocación en sus sistemas y la publicar una nueva CRL con el certificado revocado como es especificado en 4.10.1.

Inmediatamente luego de emitida la CRL se deberá enviar a la UCE.

4.9.6.Requerimientos de comprobación de revocación por terceros aceptantes

Para la validación de un certificado (ver sección 9.17.3.6), 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.

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

4.9.7.Frecuencia de emisión de CRL

Las ACPA emisora deberá cumplir los requerimientos de CABF Baseline Requirements [1] en cuanto a la frecuencia de emisión de CRL. Las ACPAs deberán publicar un CRL por lo menos cada 24 horas.

4.9.8.Latencia máxima de CRL

Un pedido de revocación recibido por una RA durante el periodo de 24 horas previo a la emisión de la próxima CRL deberá ser incluido en la misma si este fue recibido por lo menos 30 minutos antes de la emisión.

4.9.9.Disponibilidad de comprobación en línea de revocación/estado

Las ACPAs emisoras deberán proveer tiempos de respuesta menor a 10 segundos bajo condiciones normales de la red para los servicios de OCSP y CRL.

4.9.10.Requerimientos de comprobación de revocación en linea

Los terceros aceptantes deberán confirmar la información de revocación.

4.9.11.Otras formas de publicidad de revocación disponibles

No estipulado.

4.9.12.Requerimientos especiales en relación con compromiso de claves

La ACPA emisora y sus RA deberán usar métodos comercialmente razonables para informar a sus suscriptores que su clave privada a sido comprometida. Esto incluye casos donde nuevas vulnerabilidades fueron descubiertas o donde la ACPA emisora bajo su propia discreción decide que hay evidencia que sugiere un posible compromiso de la clave. Cuando el compromiso de la clave es evidente la ACPA emisora deberá revocar

los certificados asociados a la clave privada y publicar una CRL revisada en menos de 24 horas.

4.9.13.Circunstancias para la suspensión

No se soportará la suspensión de certificados.

4.9.14.Quién puede solicitar la suspensión

No es aplicable.

4.9.15.Procedimiento para la solicitud de suspensión

No es aplicable.

4.9.16.Limites del periodo de suspensión

No es aplicable.

4.10.Servicios de estado de certificados

4.10.1.Características operacionales

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

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

1. se produzca la revocación de un certificado, con un margen de tiempo de 2 horas luego de la revocación;

2. 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.

4.10.2.Disponibilidad del servicio

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

4.10.3.Características opcionales

No estipulado.

4.11.Fin de la suscripción

El fin de la suscripción ocurre en las siguientes situaciones:

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

4.12.Custodia y recuperación de claves

No se encuentra permitido realizar archivado (*escrow*) de la clave del Suscriptor para Certificados de Servidor SSL/TLS.

4.12.1.Políticas y practicas de custodia y recuperación de claves

No es aplicable.

4.12.2.Políticas y practicas de encapsulamiento y recuperación de claves de sesión

No es aplicable.

5.Gestión de las instalaciones y controles operacionales

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 prejuicio 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:

- la información personal del suscriptor actual y anteriores si hubiese;
- los trámites de solicitud, renovación o revocación de certificados;
- La clave privada del certificado emitido –en caso que la generación la realice el PSCA-;
- los documentos internos del PSCA, que describen los procesos operativos y los controles de seguridad implementados;
- los registros de auditoría impresos o en sistemas informáticos; y,
- la 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 físicos

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:

1. Controles para el acceso físico del personal a las instalaciones;
2. Definición de perímetros de seguridad en función de la criticidad de la información;
3. Inventario de activos físicos de información y controles periódicos de inventario;
4. Controles para el ingreso y egreso de activos físicos de información;
5. Controles para la protección de la infraestructura contra incendios e inundaciones;
6. Controles para la protección contra factores climáticos tales como humedad y temperatura;
7. Procedimiento para disposición de información.

5.1.1. Localización del sitio y construcción

La ACPA emisora deberá asegurar que las instalaciones donde se procesa información critica y sensible están localizadas en áreas seguras con adecuada seguridad física y control de acceso.

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 [4].

5.1.2. Acceso físico

La ACPA emisora deberá asegurar que las instalaciones usadas para la gestión del ciclo de vida de certificados son operadas en un ambiente físicamente protegido de accesos no autorizados al sistema o los datos.

5.1.3. Energía y aire acondicionado

La ACPA emisora deberá asegurar que las provisiones de energía y aire acondicionados son suficientes para el correcto funcionamiento del ACPA.

5.1.4. Exposición del agua

La ACPA emisora deberá asegurar que sus sistemas están protegidos a la exposición del agua.

5.1.5. Prevención y protección contra incendios

La ACPA emisora deberá asegurar que sus sistemas están protegidos con un sistema de extinción de incendios.

5.1.6. Almacenamiento de medios

La ACPA emisora deberá asegurar que todos los medios usados serán propiamente tratados para prevenir daños, robo y acceso no autorizado. Los procedimientos de gestión de medios deberán ser tal que estén protegidos contra obsolescencia y deterioro del medio dentro de un periodo definido y los registros que se requiere retener. Todos los medios deberán ser tratados de manera segura de acuerdo a los requerimientos del esquema de clasificación de la información de activos y los medios que contengan información sensible deberán ser seguramente desechados cuando ya no sean requeridos.

5.1.7. Eliminación de residuos

La ACPA emisora deberá asegurar que todos los medios utilizados para almacenar información son desclasificados o destruidos de una manera generalmente aceptada antes de ser liberados para su eliminación.

5.1.8. Respaldo fuera de las instalaciones

La ACPA emisora deberá asegurar que los respaldos completos de los sistemas de emisión de certificados son suficientes para la recuperación de fallos del sistema y son hechos periódicamente (el periodo deberá ser definido en las CPS). Se deberán realizar con regularidad respaldos de software e información de negocio esencial. Se deberá

contar con instalaciones que permitan la recuperación de software e información de negocio esencial.

5.2. Controles de procedimiento

5.2.1. Roles de confianza

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

1. Custodio de clave;
2. Oficial de Seguridad; y,
3. 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. 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.

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

5.2.2. Número de personas requerido por tarea

Para el procedimiento de activación de claves 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.

5.2.3. Identificación y autenticación para cada rol

Quienes desempeñen el rol de Custodio de clave tienen asignada la responsabilidad de proteger la clave privada de la ACPA, 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.

5.2.4. Roles que requieren separación de funciones

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

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.

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

5.3.Controles de personal

5.3.1.Requerimientos de calificaciones, experiencia y habilitación

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:

1. Ingreso de personal (políticas de selección, evaluación e inducción);
2. 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.);
3. Capacitación del personal (capacitación inicial y capacitaciones periódicas por rol, material utilizado para capacitación, planes de entrenamiento);
4. Retiro temporal o definitivo del personal (bloqueo o eliminación de sus cuentas de usuario);
5. Políticas para el trabajo de personal contratado (externo a la ACPA);
6. 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.).

5.3.2.Procedimiento de revisión de antecedentes

Todo el personal de la ACPA que ocupe roles de confianza debe estar libre de conflicto de intereses que puedan perjudicar la imparcialidad de las operaciones del ACPA. La ACPA no podrá designar personas a los roles de confianza que hayan sido condenados por un crimen serio u otra ofensa que pueda afectar su idoneidad para el cargo. El personal no podrá acceder a los roles de confianza hasta haberse completado todos los

chequeos necesarios. El PSCA podrá exigir los antecedentes a los candidatos y ante la negativa rechazar la solicitud para el cargo.

Todas las personas que ocupen roles de confianza deben ser seleccionados basándose en la lealtad, confianza e integridad de las mismas y deberán investigarse sus referencias y antecedentes laborales.

5.3.3. Requerimientos de capacitación

Las ACPAs emisoras debe asegurar que todo el personal realizando tareas con relación a la operación de la ACPA recibe capacitación comprensiva en:

- Principios y mecanismos de seguridad de la ACPA/RA.
- Versiones de software en uso por el sistema del ACPA
- Tareas que se espera que realice.
- Procedimientos de recuperación de desastres y continuación del negocio.

5.3.4. Requerimientos y frecuencia de actualización de capacitación

El personal de la ACPA y RA deberá ser re-capacitado cuando haya cambios en la operación de los sistemas del ACPA y RA. La re-capacitación debe ser realizada cuando sea requerido y la PSCA debe de revisar los requerimientos de re-capacitación por lo menos una vez al año.

Los individuos responsables de roles de confianza deberán estar al tanto de los cambios en la operación de los sistemas del ACPA y RA cuando sea aplicable. Cualquier cambio significativo en las operaciones debe tener su plan de capacitación y la ejecución de dicho plan debe de estar documentado.

5.3.5. Secuencia y frecuencia de rotación laboral

Las ACPAs emisoras deben asegurar que cualquier cambio en el staff no afectará la efectividad operacional del servicio ni la seguridad del sistema.

5.3.6. Sanciones por acciones no autorizadas

Sanciones disciplinarias apropiadas deben ser aplicadas al personal que viole las provisiones y políticas comprendidas en los procedimientos relacionados con la CP, CPS o el ACPA.

5.3.7. Requerimientos para contratista independiente

Las ACPAs que contraten personal independiente deben estar sujetos a los mismos procesos, procedimientos, evaluaciones, controles de seguridad y capacitaciones que el personal permanente.

5.3.8. Documentación proporcionada al personal

Los PSCA deben hacer disponible a su personal la presente política, toda CPS correspondiente y cualquier estatuto, política o contrato relevante. Otros documentos técnicos, operacionales o administrativos (Manual del administrador, Manual de usuario, etc.) son provistos a el personal de confianza para que realicen sus tareas. Se debe mantener documentado la capacitación recibida por el personal así como el nivel de la misma.

5.4. Procedimiento de registro 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.

5.4.1. Tipos de eventos registrados

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

1. registro y procesamiento de solicitudes;
2. emisión, renovación y revocación de certificados en la ACPA;
3. generación de la clave privada -en caso de que aplique-;
4. firma del acuerdo del suscriptor por parte del solicitante/suscriptor.

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.

5.4.2. Frecuencia del procesamiento del registro

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

5.4.3. Periodo de retención para el registro de auditoria

Los registros de auditoría deberán ser mantenidos por un periodo de tiempo apropiado para proveer la necesaria evidencia legal de acuerdo a toda legislación aplicable.

5.4.4. Protección del registro de auditoría

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.

Es clave la protección de la integridad y disponibilidad de los registros generados, por lo tanto los mismos deben ser almacenados de tal manera que no puedan ser destruidos ni borrados (a excepción de la transferencia a un medio de larga vida) por cualquier periodo de tiempo que se requiera retenerlos.

Los eventos deben ser almacenados de tal manera que solo el acceso de confianza autorizado es capaz de realizar operaciones de acuerdo a su perfil sin modificar la integridad, autenticidad ni confidencialidad de los datos.

Los eventos deben ser protegidos de manera que puedan ser leídos en el momento de su almacenamiento.

Los eventos deberán tener una marca de tiempo segura de tal manera que se garantice desde la fecha de creación del evento hasta el fin de su periodo de archivo, que hay una conexión segura entre el evento y la fecha de su realización.

5.4.5. Procedimiento de respaldo del registro de auditoría

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.

5.4.6. Sistema de recopilación de archivo de auditoría (interno y externo)

El sistema de recolección de registros de auditoria puede ser un componente interno. Los procesos de auditoria deben ser invocados al inicializarse el sistema y podrán terminar únicamente al apagar el sistema. El sistema de recolección de registros de auditoria debe asegurar la integridad y la disponibilidad de los datos recolectados. Si es necesario, el sistema de recolección de registros de auditoria debe proteger la confidencialidad de los datos. En el caso de la ocurrencia de un problema durante la recolección de registros de auditoría la ACPA deberá determinar si es necesario suspender las actividades del ACPA hasta que el problema haya sido solucionado, debiendo informar a los propietarios de los activos afectados.

5.4.7. Notificación al sujeto causante del evento

No estipulado.

5.4.8. Evaluación de vulnerabilidades

La ACPA debe realizar evaluaciones de vulnerabilidades regularmente cubriendo todos los activos relacionados a los productos y servicios de emisión de certificados. Las evaluaciones deben tener foco en las amenazas internas y externas que pueden resultar en acceso no autorizado, manipulación, modificación, alteración o destrucción del proceso de emisión de certificados.

5.5. Archivo de registros

En esta sección el término o archivo refiere a archivo como conjunto de documentos y no a el archivo electrónico.

5.5.1. Tipos de registros archivados

La ACPA y RA debe archivar registros con suficiente detalle para establecer la validez de una firma y la correcta operación del sistema del ACPA. Como mínimo, la siguiente información debe ser archivada:

Eventos de la gestión del ciclo de vida de la clave de la CA , incluyendo:

- Generación, respaldo, almacenamiento, recuperación, archivo y destrucción de clave;
- Eventos de la gestión del ciclo de vida del dispositivo criptográfico; y
- Configuración del equipamiento del sistema del ACPA .

Eventos de la gestión del sistema de emisión de la ACPA incluyendo:

- Acciones de inicialización y apagado del sistema;
- Intentos de crear, remover, o establecer contraseñas o cambiar el sistema; y
- Cambios en las claves del ACPA.

Eventos de la gestión del ciclo de vida del certificado del ACPA y del suscriptor, incluyendo:

- Solicitudes, renovación y reasignación de claves del Certificado, y revocación para tanto los intentos satisfactorios como los no satisfactorios;
- Todas las actividades de verificación estipuladas en la presente política;
- Fecha, hora, numero de teléfono usado, personas con las que se hablo y resultados finales de las llamadas telefónicas de verificación;
- Aceptación y rechazo de las solicitudes de Certificados;
- Emisión, revocación y expiración de Certificados; y
- Generación de CRLs y entradas OCSP incluyendo operaciones de lectura-y-escritura fallidas en el directorio de certificados y CRLs.

Eventos de seguridad, incluyendo:

- Intentos de acceso satisfactorios e insatisfactorios al sistema PKI;
- Acciones de sistema de seguridad y PKI realizadas;
- Cambios en el perfil de seguridad;

- Fallos del sistema, fallos de hardware y otras anomalías;
- Actividades de Firewall y de enrutadores; y
- Entradas y salidas de las instalaciones del ACPA.

Documentación y auditoría:

- Documentación de auditoría incluyendo todas las comunicaciones relacionadas con el trabajo entre la ACPA y los auditores;
- Políticas de certificación y versiones previas;
- Declaración de Practicas de Certificación y versiones previas; y
- Acuerdos contractuales entre los Suscriptores y la ACPA emisora

Sellado de tiempo:

- Sincronización de reloj

Misceláneas

- Otros datos o aplicaciones suficientes para verificar contenidos de archivos;
- Fallos de equipamiento;
- Fallos de UPS o apagones eléctricos; y
- Violaciones a esta CP o CPS.

5.5.2. Periodo de retención para el archivo

El mínimo periodo de retención de datos de archivo debe ser de 10 años.

5.5.3. Protección del archivo

Los archivos deberán ser creados de tal manera que no puedan ser destruidos ni borrados (a excepción de la transferencia a un medio de larga vida) por cualquier periodo de tiempo que se requiera retenerlos.

Los eventos deben ser almacenados de tal manera que solo el acceso de confianza autorizado es capaz de realizar operaciones de acuerdo a su perfil sin modificar la integridad, autenticidad ni confidencialidad de los datos.

Los eventos deben ser protegidos de manera que puedan ser leídos en el momento de su almacenamiento.

Los eventos deberán tener una marca de tiempo segura de tal manera que se garantice desde la fecha de creación del evento hasta el fin de su periodo de archivo, que hay una conexión segura entre el evento y la fecha de su realización.

5.5.4. Procedimientos de respaldo del archivo

No estipulado.

5.5.5. Requerimientos para el sellado de tiempo de los registros

Si se utiliza un servicio de sellado de tiempo para fechar los registros, entonces deberá respetar los requerimientos definidos en la sección 6.8. Independientemente del método de sellado de tiempo, todos los registros deben contar con información que indique cuando ocurrió el evento.

5.5.6. Sistema de recopilación de archivo (interno o externo)

El sistema de recopilación de archivo puede ser un componente interno. El sistema de recopilación de archivo debe asegurar la integridad y la disponibilidad de los datos recolectados. Si es necesario, el sistema de recopilación de archivo debe proteger la confidencialidad de los datos.

5.5.7. Procedimientos para obtener y verificar la información del archivo

Los medios de almacenamiento utilizados por el ACPA para el almacenamiento de archivo son chequeados al momento de la creación. Periódicamente, muestras estadísticas de la información archivada son probadas para comprobar la integridad y

legibilidad de la información. Solo el equipamiento del ACPA, roles de confianza y otras personas autorizadas se les permite acceder al archivo.

5.6. Cambio de clave

No es aplicable.

5.7. Compromiso y recuperación de desastres

5.7.1. Procedimientos de manejo de incidentes y compromisos

Deben establecerse procedimientos que permitan la recuperación de los sistemas, continuidad de las operaciones y la protección de la información en caso 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 4.9).

Deben abordarse mínimamente los siguientes requerimientos:

1. Políticas para identificación de incidentes que puedan ocasionar un desastre en la operativa de la ACPA;
2. Procedimientos de recuperación para infraestructura y software en el caso de corrupción de datos;
3. Procedimientos para actuar en el caso de que la clave privada de la ACPA haya sido comprometida o se sospeche de su compromiso;
4. Procedimientos para la protección de la información y continuidad de las operaciones en el caso de un desastre natural (inundación, incendio, derrumbe, etc.).

5.7.2. Corrupción de recursos de computo, datos y/o software

Si algún equipo es dañado o queda inoperativo, pero las claves de firma no son destruidas, la operación deberá ser reestablecida lo antes posible, dando prioridad a la habilidad de generar información de estado de certificados de acuerdo al plan de recuperación de desastres de la ACPA.

5.7.3. Procedimientos ante el compromiso de clave privada de entidad

En caso que la clave privada de un ACPA sea comprometida, perdida, destruida o se sospecha que haya sido comprometida, la ACPA deberá, luego de investigar el problema, decidir si el certificado del ACPA debe ser revocado. Si debe ser revocado:

- Todos los suscriptores a quienes se les haya emitido un certificado serán notificados lo antes posible.
- Se generará un nuevo par de llaves para el ACPA o un ACPA alternativo se usará para crear nuevos Certificados de servidor SSL/TLS

5.7.4. Capacidades de continuidad de negocio después de un desastre

El plan de recuperación de desastres prevé la continuidad del negocio como es especificado en 5.7.1. Los sistemas de información de estado de los Certificados deberán ser desplegados de manera que haya disponibilidad las 24 horas del día, los 365 días del año (con una razón del 99,95% de disponibilidad excluyendo las operaciones de mantenimiento programada).

5.8. Terminación de la CA o de la RA

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 servidor SSL/TLS. En ambos casos, los PSCA deberán realizar la terminación de las operaciones de sus ACPA de acuerdo con las regulaciones establecidas por la UCE.

5.9. Procedimiento para el cambio de certificado de la ACPA

Según la Política de Certificación de la ACRN [4], 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.

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 prejuicio 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.Generación e instalación del par de claves

6.1.1.Generación del par de claves

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 [4].

La ACPA podrá generar el par de claves para validaciones totalmente presenciales, teniendo estos que ser generados siempre en un entorno físicamente seguro bajo personal con roles de confianza.

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.

6.1.2.Entrega de la clave privada al suscriptor

Las ACPAs que generen la clave privada en nombre de los suscriptores lo podrán realizar únicamente cuando se mantenga seguridad suficiente desde el proceso de generación de claves en adelante hasta cualquier proceso de emisión al suscriptor.

Esto incluye la capacidad de garantizar la integridad de la clave, la aleatoriedad de la clave a través de generadores de números aleatorios o pseudo-aleatorios y la elección de un mecanismo de encriptación adecuado para el transporte de la clave al suscriptor.

El ACPA emisora no deberá archivar claves privadas y debe asegurar que cualquier localidad temporal de la clave en cualquier lugar de memoria utilizado durante la generación de la clave sea borrado.

6.1.3. Entrega de la clave pública al emisor del certificado

La ACPA emisora deberá aceptar únicamente claves públicas que han sido protegidas en su transito y provenientes de RAs, verificándose la autenticidad y la integridad de su origen de la RA. Las RAs deberán aceptar únicamente claves publicas de los suscriptores en linea con los requerimientos de la sección 3.2.1 de la presente política.

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

La ACPA emisora debe asegurar que la entrega de la claves públicas a los terceros aceptantes es hecha de tal manera que prevenga ataques de substitución. Las claves públicas generadas por la ACPA emisora podrán ser entregadas al suscriptor por medio de una cadena de certificados o a través de un repositorio gestionado por el ACPA emisora y referenciado en el perfil del certificado emitido.

6.1.5. Tamaños de clave

La ACPA debe seguir las recomendaciones y mejores practicas del NIST con respecto a la elección del material de las claves.

Los siguientes tamaños de claves y algoritmos de hash deberán usarse como mínimo para los certificados emitidos y los respondedores de estado de Certificado CRL/OCSP siguiendo los requerimientos del CABF Baseline Requirements [1] :

- 2048 bit como mínimo para claves RSA con algoritmo de hash SHA-256 o superior
- 256 bits como mínimo para claves ECDSA con algoritmo de hash SHA-256 o superior

Cuando sea posible, toda la cadena de certificados y cualquier respuesta de estado de certificado usará el mismo nivel de seguridad y criptografia.

6.1.6. Generación y control de calidad de parámetros de clave pública

El ACPA emisora deberá generar claves en cumplimiento con FIPS 186 y deberá usar técnicas razonables para validar la aplicabilidad de las claves presentadas por los suscriptores. Se deberá verificar si la clave es una clave débil conocida y rechazarla al momento de sumisión.

6.1.7. Propósitos de uso de la clave (por campo Key Usage de certificado X.509 v3)

Los campos Key Usage para los Certificados de Servidor SSL/TLS serán:

- DigitalSignature
- ContentCommitment
- KeyEncipherment
- KeyAgreement

como es especificado en el punto 7.1.2.

6.2. Protección de la clave privada y controles de ingeniería del módulo criptográfico

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 [4].

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

La clave privada, cuando no esté siendo utilizada, debe encontrarse desactivada. La misma será protegida con 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.

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

6.2.1. Normas y controles para el módulo criptográfico

Si el ACPA emisora requiere que sus suscriptores utilicen sistemas FIPS 140-2 nivel 2 o superiores para la protección de la clave privada, deberá obligar al suscriptor contractualmente de usar ese sistema o proveer un mecanismo para garantizar la protección. Esto podrá ser logrado por ejemplo mediante la limitación a un CSP (Cryptographic Service Provider) particular ligado a una plataforma conocida de hardware compatible con FIPS como parte del proceso de inscripción.

6.2.2. Control multi-persona (m de un total de n) de la clave privada

La ACPA emisora deberá activar la clave privada con control multi-persona (usando los datos de activación del ACPA) como es estipulado en el punto 5.2.2 . Los roles de confianza permitidos de participar en la activación de la clave deberán estar fuertemente autenticados (por ejemplo Token con código PIN).

6.2.3. Custodia de la clave privada

La ACPA emisora no podrá hacer escrow de su clave privada bajo ningún concepto.

6.2.4. Respaldo de la clave privada

La ACPA emisora podrá realizar respaldos de su clave privada bajo los mismos controles multi-persona que la clave original para el plan de recuperación de desastres.

6.2.5. Archivo de la clave privada

La ACPA emisora no debe archivar la clave privada.

6.2.6. Transferencia de la clave privada desde/hacia un módulo criptográfico

La ACPA emisora deberá generar, activar y guardar su clave privada en un HSM. Cuando la clave privada este fuera de un HSM (para almacenamiento o transferencia), deberá estar encriptada. Las claves privadas jamas deberán existir en texto plano fuera de un HSM.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

La ACPA emisora deberá almacenar su clave privada en por lo menos un dispositivo FIPS 140 nivel 3.

6.2.8. Método de activación de la clave privada

La ACPA emisora será responsable de activar la clave privada de acuerdo a las instrucciones y documentación provista por el proveedor del HSM. Los suscriptores son responsables de proteger sus claves privadas conforme con las obligaciones que son presentadas en el acuerdo de suscriptor.

6.2.9. Método de desactivación de la clave privada

La ACPA emisora deberá asegurar que los HSM que hayan sido activados no sean desatendidos o disponibles a acceso no autorizado. Durante el tiempo que el HSM de un ACPA se encuentre en linea y operacional será usado únicamente para firmar certificados y CRL/OCSPs de una RA autenticada. Cuando una ACPA no este operacional, sus claves privadas serán removidas del HSM.

6.2.10. Método de destrucción de la clave privada

Las claves privadas de la ACPA deberán ser destruidas cuando ya no se necesiten o cuando los certificados correspondientes hayan expirado o hayan sido revocados. Al destruir las claves privadas la ACPA emisora deberá destruir todo los datos secretos de activación asociados a la clave, de tal manera que no se pueda usar información para deducir parte alguna de la clave privada.

6.2.11. Clasificación del modulo criptográfico

Ver sección 6.2.1.

6.3.Otros aspectos de la gestión del par de claves

6.3.1.Archivo de clave pública

La ACPA emisora deberá archivar las claves publicas de los certificados.

6.3.2.Periodos operacionales del certificado y periodos de uso del par de claves

Los certificados del ACPA emisora y los certificados renovados deberán tener un periodo máximo de validez de:

Tipo	**Terminación del certificado**
Certificado de la ACRN	20 años
Certificado de un ACPA	Máximo tiempo según vigencia del certificado de la ACRN al momento de la emisión
Certificado de Servidor SSL/TLS	39 meses

6.4.Datos de activación

6.4.1.Generación e instalación de los datos de activación

La generación y uso de los datos de activación del ACPA emisora usados para activar las claves privadas del ACPA, deberán realizarse durante la ceremonia de claves. Los datos de activación deberán ser generados automáticamente por el HSM apropiado y entregado a una persona en un rol de confianza. El método de entrega deberá mantener la confidencialidad y la integridad de los datos de activación.

6.4.2.Protección de datos de activación

El PSCA debe proteger la clave privada y los datos de activación de la ACPA conforme se especifica en la sección 6.3 y 6.5 de la Política de Certificación de la ACRN [4].

6.4.3. Otros aspectos de los datos de activación

Los datos de activación del ACPA podrán mantenerlos únicamente personal en roles de confianza.

6.5. Controles de seguridad computacional

6.5.1. Requerimientos técnicos específicos de seguridad computacional

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 [4].

6.5.2. Clasificación de la seguridad computacional

No estipulado.

6.6. Controles técnicos de ciclo de vida

6.6.1. Controles de desarrollo de sistema

No estipulado.

6.6.2. Controles de gestión de la seguridad

No estipulado.

6.6.3. Controles de seguridad del ciclo de vida

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 [4].

6.7. Controles de 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 [4].

6.8. Sellado de tiempo

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 [4].

7.Perfiles de Certificado y CRL

El formato de los certificados de Servidor SSL/TLS deben cumplir con lo especificado en:

- El estándar ITU-T X.509 [8].
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Abril 2002 ("RFC 5280") [9]
- La versión actual de CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [1].

La lista de revocación de certificados debe cumplir con el estándar ITU-T X.509, pero en su versión 2 como es estipulado en el RFC 5280 ademas de cumplir con los CABF Baseline Requirements.

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

7.1.Perfil del certificado de Servidor SSL/TLS

Como mínimo los certificados de servidor SSL/TLS deberán tener los siguientes campos básicos del formato X.509 versión 3 [8]:

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACPA emisora no secuencial con 20 bits de entropía por lo menos.
Algoritmo de Firma (Signature Algorithm)	OID del algoritmo usado para firmar el certificados como es especificado en el punto 7.1.3.
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA emisora tal cual figura en su certificado.
Validez (Valid From / Valid To)	0 a 39 meses (en formato desde/hasta)
Nombre Distintivo del Suscriptor	DN del suscriptor como es estipulado en 3.1.1.

(Subscriber DN)	
Clave Pública del Suscriptor (Subject Public Key)	Clave pública. En el caso de ser una clave RSA deberá ser de 2048 bits o más y el exponente público deberá ser un numero impar entre (2^16)+1 y (2^256)-1. El módulo deberá tener las siguientes características: Número impar, que no sea potencia de un primo, y que no tenga factores menores a 752. Si la clave es ECC se deberá usar alguna de las siguientes curvas: P-256, P-384, o P-521. La ACPA deberá confirmar la validez de toda clave usando el "ECC Full Public Key Validation Routine" o bien el "ECC Partial Public Key Validation Routine".

7.1.1. Número(s) de versión

Los certificados emitidos bajo esta política son certificados X.509 versión 3 [8].

7.1.2. Extensiones del certificado

Los certificados emitidos bajo la presente política contendrán las siguientes extensiones:

Campo	Critico	Valor
Identificador de la clave del suscriptor (Subject Key Identifier)	FALSE	Hash de 20 bytes del atributo Subject Public Key
Identificador de la clave de la autoridad (Authority Key Identifier)	FALSE	Valor de la Extensión Subject Key Identifier del certificado de la ACPA emisora
Uso de Claves (Key Usage)	TRUE	DigitalSignature = 1 NonRepudiation/contentCommitment = 1 KeyEncipherment = 1 DataEncipherment = 0 KeyAgreement = 1 KeyCertSign = 0 CRLSign = 0

		EncipherOnly = 0 DecipherOnly = 0
Uso de Claves Extendido (Extended Key Usage)	FALSE	clientAuth serverAuth
Políticas de Certificación (Certificate Policies)	FALSE	Policy Qualifier Policy Qualifier ID (OID): 2.16.858.10000157.66565.9 CPS Pointer: http://www.uce.gub.uy/informacion-tecnica/politicas/cp_servidor_ssl_tls.pdf Policy Qualifier Policy Qualifier ID (OID): OID asignado a la CPS del PSCA para la ACPA emisora CPS Pointer: URL de publicación de la CPS User Notice qualifier: Opcionalmente se podrá incluir un aviso al usuario relativo a las condiciones de uso del certificado por parte del tercero aceptante. Si la validación del suscriptor fue mediante "Validación de Dominio": Policy Identifier (OID): {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1) Si la validación del suscriptor fue mediante "Validación Organizacional": Policy Identifier OID: {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) subject-identity-validated(2)} (2.23.140.1.2.2)
Restricciones Básicas (Basic Constraints)	TRUE	CA = FALSE

Puntos de distribución de las CRL (CRL Distribution Points)	FALSE	URI = URL primaria de publicación de la CRL URI = URL secundaria de publicación de la CRL
Nombre alternativo del suscriptor (Subject alternative name)	FALSE	Aquí se colocaran todos los nombres de dominio o direcciones IP validados que se desee incluir como es estipulado en 3.1.1.
Información de Acceso de la Autoridad Certificadora	FALSE	URL del certificado de la ACPA emisora URL del servicio OCSP, si es que la ACPA lo tiene

7.1.3. Identificadores de objeto de algoritmos

La ACPA emisora deberá firmar los certificados de servidor SSL/TLS con alguno de los siguientes algoritmos:

Sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11 }
Sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12 }
Sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 10 }

Si una ACPA emisora firma certificados usando RSA con “PSS padding”, la CA emisora podrá usar los siguientes algoritmos y OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Los suscriptores podrán generar pares de claves usando lo siguiente:

RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) idpublicKeyType(2) 1 }

7.1.4. Formas de nombre

Los certificados de servidor SSL serán completados con un nombre de emisor y un nombre distinguido del sujeto de acuerdo a la sección 3.1.1 utilizando atributos estándar como los identificados en el RFC5280 [9].

El Nombre del Emisor deberá ser completado en cada certificado emitido conteniendo el mismo nombre distinguido que utiliza en su certificado.

La CA emisora incluirá en cada certificado un único número de serie no secuencial con por lo menos 20 bits de entropía.

La CA emisora restringirá campos OU que contengan información del suscriptor que no se verifica en conformidad con la sección 3.2.

Se completará la extensión Subject Alternative Name como es indicado en el punto 3.1.1.

7.1.5. Restricciones de nombres

No es aplicable. Los certificados finales no utilizan la extensión Name Constraints.

7.1.6. Identificadores de objeto de política de certificación

En la extensión Certificate Policies se utilizaran los OID de las siguientes políticas:

{ joint-iso-ccitt(2) country(16) uy(858) ince(10000157) policy(66565) 9 }	La presente política de certificación.
{ joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)}	Este OID se utilizará cuando se haya realizado una validación de dominio del suscriptor, este OID indica que se siguieron los lineamientos del “CAB Forum Guidelines” para validación de dominio (DV).
{ joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) subject-identity-validated(2)}	Este OID se utilizará cuando se haya realizado una validación de identidad de tipo organizacional del suscriptor, este OID indica que se siguieron los lineamientos del “CAB Forum Guidelines” para validación de organizacional (OV).

Los certificados emitidos bajo la presente política contendrán o bien el identificador correspondiente a dominio validado o a organización validada dependiendo el tipo de validación realizada conforme al punto 3.2.

Adicionalmente se utilizará el OID correspondiente a las CPS de la CA emisora, como esta estipulado en el esquema 7.1.2.

7.1.7. Uso de la extensión "Policy Constraints"

No es aplicable. No se utiliza la extensión Policy Constraints en certificados finales.

7.1.8. Sintaxis y semántica de calificadores de política

Se utilizarán los calificadores definidos en el RFC5280 [9]. Particularmente se utilizará el calificador "CPS Pointer qualifier" donde se colocara la URI en la que se accede al documento y el calificador "User Notice Qualifier" donde se podrá incluir un aviso al usuario acerca de las condiciones de uso del certificado, por ejemplo que cualquier uso del certificado constituye la aceptación de las practicas de certificación y del acuerdo del tercero aceptante.

7.1.9. Semántica de procesamiento para la extensión critica "Certificate Policies".

No es aplicable. La extensión Certificate Policies no se marca como critica.

7.2. Perfil de la CRL de las ACPA de PSCA

Se utilizarán los siguientes campos del formato X.509 versión 2 [8]:

Atributos	Contenido
Versión (Version)	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA tal cual figura en su certificado
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 ACPA
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

8.Auditoria de cumplimiento y otras evaluaciones

8.1.Frecuencia o circunstancias de evaluación

Los requerimientos de auditoría de la UCE se encuentran estipulados en la Política de Certificación de la ACRN [4].

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.

Independientemente de los requerimientos de auditoria estipulados por la UCE, los PSCA que pretendan emitir certificados de servidor SSL/TLS bajo la presente política, deberán someterse a auditorias al menos anualmente, tal como lo requieren los CABF Baseline Requirements.

8.2.Identidad/calificaciones del evaluador

Por resolución de la UCE N° 001/2012 se establecen requerimientos para dar carácter de auditor autorizado a los evaluadores que pretenden realizar las auditorias sobre los PSCA. La lista de evaluadores habilitados se encuentra publicada en el sitio web de la UCE (www.uce.gub.uy).

8.3.Relación del evaluador con la entidad evaluada

El evaluador deberá ser un auditor independiente.

8.4.Tópicos cubiertos por la evaluación

Las auditorías realizadas sobre los PSCA que emitan certificados de servidor SSL/TLS deben de cumplir con los requerimientos del esquema de auditoria de la UCE, así como también los CABF Baseline Requirements.

8.5.Acciones a tomar como resultado de la deficiencia

En caso de deficiencias, se deberá crear un plan de acción correctivo para remover la deficiencia y presentarlo ante la UCE, quien podrá tomar las acciones que considere apropiadas dependiendo de la importancia de las deficiencias.

8.6.Comunicación de los resultados

Los resultados de las auditorias deberán ser presentados ante la UCE para el análisis y resolución de cualquier deficiencia a través de un posterior plan de acción correctivo.

9.Otros aspectos comerciales y legales

9.1.Tarifas

9.1.1.Tarifas de emisión o renovación de certificados

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

9.1.2.Tarifas de acceso a los certificados

No estipulado.

9.1.3.Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados deberá ser gratuita.

9.1.4.Tarifas para otros servicios

No estipulado.

9.1.5.Política de reembolsos

No estipulado.

9.2.Responsabilidad financiera

La responsabilidad financiera se regulará por la normativa nacional vigente.

9.2.1. Cobertura de seguros

A los efectos de la cobertura de seguros deberá estarse a lo establecido en la normativa legal, reglamentaria y regulatoria vigente.

9.2.2. Otros activos

No estipulado.

9.2.3. Garantía o cobertura de seguro para entidades finales

No estipulado.

9.3. Confidencialidad de la información de negocios

9.3.1. Alcance de la información confidencial

El carácter confidencial de la información se regirá de acuerdo con el marco normativo vigente.

La información confidencial queda regulada por las Leyes Nos. 18.331, de 8 de agosto de 2008, 18.381, de 17 de octubre de 2008, sus correspondientes decretos reglamentarios, modificaciones y demás normas concordantes.

La información que la UCE publica sobre los PSCA se encuentra estipulada en la Política de Certificación de la ACRN [4].

9.3.2. Información fuera del alcance de la información confidencial

La información sobre la revocación de los certificados de Servidor SSL/TLS, no se considera confidencial y será publicada por los PSCA mediante las CRL y servicios OCSP 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 4.9.5.

9.3.3. Responsabilidad de proteger la información confidencial

La responsabilidad en la protección de la información confidencial se regulará por la normativa nacional vigente.

9.4. Confidencialidad de la información personal

La determinación del carácter confidencial de la información se regulará de acuerdo con el marco normativo vigente.

9.4.1. Plan de privacidad

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

9.4.2. Información personal

La información personal queda regulada de acuerdo con lo dispuesto por las Leyes Nos. 18.331, de 8 de agosto de 2008 y 18.381, de 17 de octubre de 2008, sus correspondientes decretos reglamentarios, normas modificativas y concordantes.

Debe considerarse incluida en ésta, toda la información de los suscriptores que no aparezca en los certificados, en cumplimiento de la normativa nacional vigente.

Asimismo, la información relativa al suscriptor que describa su infraestructura tecnológica o de procesos internos de negocio se considera incluida en el concepto y por tanto generarán responsabilidades vinculadas con la información personal.

Deberá entrenarse al personal de la autoridad de registro a los efectos que verifiquen especial cuidado en su tratamiento.

9.4.3. Información pública

De acuerdo con lo establecido en la Ley Nº 18.381, de 17 de octubre de 2008, la información puede revestir el carácter de pública, secreta por Ley, reservada y confidencial. En ese marco, de principio toda la información es pública, salvo aquélla especialmente determinada como secreta por Ley, reservada y confidencial.

9.4.4. Responsabilidad de proteger información personal

La responsabilidad en la protección de la información confidencial se regulará por la normativa nacional vigente.

Las ACPAs son responsables de almacenar de forma segura la información personal de acuerdo con el documento de Política de Privacidad Público.

9.4.5. Aviso y consentimiento de usar información personal

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 previo consentimiento del titular.

No se requerirá autorización previa cuando la información haya sido obtenida de fuentes de acceso público.

9.4.6. Divulgación de conformidad con proceso judicial o administrativo

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

9.4.7. 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.

9.5.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.

9.6.Declaraciones y garantías

9.6.1.Declaraciones y garantías de la CA

Las garantías se regirán por lo dispuesto en la normativa nacional vigente.

Sin perjuicio de lo señalado, la CA podrá realizar una declaración en relación con la utilización de los certificados debiendo siempre resguardarse la integridad de la clave privada.

En caso de existir sospechas en relación con el compromiso de la misma, deberá procederse de acuerdo con lo estipulado en la Ley Nº 18.600 y el Decreto Nº 436/011.

9.6.2.Declaraciones y garantías de la RA

Las garantías se regirán por lo dispuesto en la normativa nacional vigente.

9.6.3.Declaraciones y garantías del suscriptor

Sin perjuicio de lo establecido en la normativa vigente, los suscriptores son responsables de:

A) Brindar declaraciones exactas y completas en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación.

B) Mantener el control exclusivo de sus datos de creación de firma electrónica avanzada, no compartirlos e impedir su divulgación.

C) Utilizar un dispositivo de creación de firma electrónica avanzada técnicamente confiable.

D) Solicitar la revocación de su certificado reconocido al prestador de servicios de certificación acreditado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma.

E) Informar sin demora al prestador de servicios de certificación acreditado el cambio de alguno de los datos contenidos en el certificado reconocido que hubiera sido objeto de verificación.

9.6.4. Declaraciones y garantías del tercero aceptante

El tercero aceptante que hiciere uso de un certificado, asume la carga de comprobar que:

A) El certificado es válido y fue emitido por un PSCA de la INCE.

B) La fecha de validación del certificado debe ser posterior a la fecha de entrada en vigencia del certificado y anterior a la de expiración.

C) El certificado no se encuentra revocado en la última CRL emitida por el PSCA a la fecha de la validación, o el servicio de validación online OCSP 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.

E) El certificado de la ACRN es válido.

F) El certificado se está utilizando para uno de los usos permitidos en la Política de Certificación correspondiente.

9.6.5. Declaraciones y garantías de los demás participantes

No aplica.

9.7. Renuncia de garantías

No aplica.

9.8.Limitaciones de responsabilidad

Los PSCA responderán por los daños y perjuicios causados en razón del uso indebido del certificado reconocido cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

La responsabilidad será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda.

9.9.Indemnizaciones

En caso que la garantía constituida por los PSCA fuera insuficiente para satisfacer la indemnización debida, éstos responderán de la deuda con todos sus bienes presentes y futuros.

9.10.Vigencia y término

9.10.1.Vigencia

La presente política se encontrará vigente hasta tanto no sea sustituida, lo que será oportunamente publicitado de acuerdo con los criterios de estilo, en el Diario Oficial.

9.10.2.Término

En caso de efectuarse modificaciones parciales, éstas se indicarán de acuerdo con el versionado adecuado, sin perjuicio de la publicidad de la misma de acuerdo con los criterios de estilo en el Diario Oficial.

9.10.3.Efecto de término y sobrevivencia

No aplica.

9.11.Avisos individuales y comunicaciones con los participantes

No aplica.

9.12.Modificaciones

9.12.1.Procedimiento para cambio de especificaciones

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

9.12.2.Procedimiento de enmiendas

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.

9.12.3.Mecanismo y periodo de notificación

La notificación de las modificaciones y enmiendas se efectuará de acuerdo con lo previsto en la normativa nacional vigente y los procedimientos de estilo, en el Diario Oficial.

9.12.4.Circunstancias en las que el OID debe ser cambiado

No aplica.

9.13.Disposiciones de resolución de disputas

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.

9.14.Ley aplicable

La presente política deberá ser interpretada de acuerdo con lo establecido en la Ley Nº 18.600, de 21 de Setiembre de 2009 [3], su normativa reglamentaria, regulaciones aprobadas por la UCE, modificaciones y demás normas concordantes. En igual sentido su validez, estructura y obligatoriedad derivan de la normativa legal, reglamentaria y regulatoria vigente.

9.15.Conformidad con la ley aplicable

No aplica.

9.16.Provisiones varias

9.16.1.Acuerdo completo

No aplica.

9.16.2.Asignación

No aplica.

9.16.3.Divisibilidad

No aplica.

9.16.4.Cumplimiento (honorarios de abogado y renuncia de derechos)

No aplica.

9.16.5.Fuerza mayor

No aplica.

9.17.Otras disposiciones

9.17.1.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.

9.17.2.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.

9.17.3.Obligaciones

9.17.3.1.Obligaciones de la UCE

Las obligaciones de la UCE se encuentran especificadas en la Política de Certificación de la ACRN [4]. Además de dichas obligaciones generales, constituyen obligaciones específicas de la UCE en el contexto de la presente Política:

1. La actualización, aprobación y cancelación de la presente Política de Certificación de la INCE – PKI Uruguay;
2. La acreditación de Prestadores de Servicios de Certificación para operar dentro de la INCE emitiendo certificados de Servidor SSL/TLS;
3. La publicación de la lista de PSCA habilitados a emitir certificados de Servidor SSL/TLS dentro del contexto de la INCE;
4. Mantener a disposición permanente del público la presente Política de Certificación, tanto la versión vigente como las anteriores;

5. Atender los pedidos de revocación de certificados de Servidor SSL/TLS solicitados por una autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;

9.17.3.2. 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 [4].

9.17.3.3. 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 Servidor SSL/TLS. Constituyen obligaciones de dichos Prestadores:

1. Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, de conformidad con lo pautado en la presente Política;
2. 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 6.1.1 de la presente Política;
3. Proteger las claves privadas de sus ACPA;
4. 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 [4];
5. Solicitar a la ACRN la revocación del certificado de sus ACPA ante sospecha real de compromiso de la clave privada asociada;
6. 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;
7. Utilizar el certificado de sus ACPA de acuerdo con los requerimientos de la presente Política de Certificación;
8. La emisión, renovación y revocación de los certificados de Servidor SSL/TLS de sus suscriptores;
9. La emisión y publicación de su Lista de Certificados Revocados (CRL);
10. Informar a sus suscriptores de la revocación de sus certificados, junto con la causal para dicha operación;
11. El envío a la UCE de las CRL inmediatamente después de emitidas;
12. 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;

13. 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;
14. Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad, no repudio o confidencialidad según corresponda)

9.17.3.4.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:

1. 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;

2. Comprobar, de acuerdo con lo estipulado en el punto 3.2 y Error: No se encuentra la fuente de referencia:

3. En caso de que el solicitante sea una Persona Jurídica, la identidad de la persona jurídica para la cual será emitido el certificado, a través de certificado notarial,

4. En caso de que el solicitante sea una Persona Física, la identidad de la persona física que solicita la emisión, renovación o revocación presencial del certificado, mediante la validación del documento de identidad presentado,

5. En caso que el solicitante sea una persona jurídica, que la persona física Representante del solicitante cuente con las facultades necesarias para solicitar, renovar o revocar el certificado de la persona jurídica correspondiente.

6. Notificar a los suscriptores de certificados de Servidor SSL/TLS 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;

9.17.3.5.Obligaciones de los Suscriptores de Certificados

En el contexto de la presente Política de Certificación, los suscriptores son Personas Jurídicas o Físicas constituidas en la República Oriental del Uruguay, bajo cuya responsabilidad recaerán las obligaciones citadas en este punto.

Toda la información necesaria para la identificación y autenticación de la Persona Jurídica o Física a certificar, debe ser provista de forma completa y precisa al iniciar el proceso de registro. Dicha información y procedimiento de registro se especifica en la sección 3.2.

Al aceptar un certificado emitido por un ACPA de PSCA, el suscriptor 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.

El suscriptor debe hacer uso del certificado en conformidad con la presente Política de Certificación para certificados de Servidor SSL/TLS, con las demás Políticas de Certificación aplicables de la INCE y demás normativa vigente

Los Suscriptores de certificados de Servidor SSL/TLS asumen las siguientes obligaciones:

1. Proveer toda la información que le sea requerida de modo completo y preciso a la Autoridad de Registro a efectos de obtener el certificado emitido por el PSCA a través de su ACPA bajo la presente política de certificación;
2. Generar su clave privada en alguna de las condiciones establecidas en el punto 6.1.1;
3. Proteger su clave privada;
4. 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;
5. Utilizar el certificado de acuerdo con los requerimientos de la presente política de certificación;
6. 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;

9.17.3.6.Obligaciones de los Terceros Aceptantes

Los Terceros aceptantes tienen las siguientes obligaciones:

1. Tomar conocimiento y aceptar los términos definidos en el presente documento, incluyendo y sin limitarse a:
2. garantías y usos aceptables del certificado de las ACPA de los PSCA;
3. garantías y usos aceptables de los certificados emitidos por los PSCA a sus suscriptores;
4. obligaciones de los Terceros aceptantes.
5. Verificar la validez del certificado de la ACRN. El certificado de la ACRN es considerado válido cuando:
6. se encuentra dentro de su período de vigencia,
7. no ha sido revocado según la CRL publicada por la ACRN.
8. Verificar la validez de los certificados emitidos por la ACRN para las ACPA. El certificado es considerado válido cuando;
9. se encuentra dentro de su período de vigencia,
10. su firma electrónica puede ser verificada con la clave pública del certificado de la ACRN, y
11. no ha sido revocado según la CRL publicada por la ACRN.
12. Verificar la validez del certificado de Servidor SSL/TLS que le está siendo presentado. El certificado es considerado válido cuando:
13. se encuentra dentro de su período de vigencia,
14. no ha sido revocado según la CRL publicada por dicha ACPA.
15. Verificar que el certificado de Servidor SSL/TLS 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 Servidor SSL/TLS emitido por un PSCA a través de su ACPA a un suscriptor final.

Referencias Externas

1: CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, 2011-2013

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

3: Poder Legislativo, República Oriental del Uruguay, Ley N° 18.600 de Documento Electrónico , 21 de setiembre de 2009

4: Unidad de Certificación Electrónica, Política de Certificación de la Autoridad Certificadora Raíz Nacional, 2011

5: Poder Ejecutivo, República Oriental del Uruguay, Reglamentación del Documento Electrónico y Firma Electrónica, 8 de diciembre de 2011

6: K. Zeilenga, Ed, RFC 4514 - Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, 2006

7: R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1, 1999

8: ITU-T Study Group 17, International Standar ISO/IEC 9594-8 | Recommendation ITU-T X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2012

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