

Política de Certificación de la Autoridad Certificadora Raíz Nacional

Versión 2.2

Unidad de Certificación Electrónica

Infraestructura Nacional de Certificación Electrónica
República Oriental del Uruguay

Índice

1.	Introducción.....	9
1.1.	Descripción general	9
	Relación entre la Política de Certificación y otros documentos	13
1.2.	Nombre del documento e Identificación de la Política de Certificación	14
1.3.	Participantes de la INCE.....	14
1.3.1.	Autoridad Certificadora	14
1.3.2.	Autoridad de Registro	15
1.3.3.	Suscriptores.....	15
...1.	Prestadores de Servicios de Certificación Acreditados	15
1.3.4.	Terceros Aceptantes	16
1.3.5.	Otros participantes	16
...2.	Unidad Reguladora	16
1.4.	Uso de los certificados.....	17
1.4.1.	Usos Permitidos de los Certificados	17
1.4.2.	Restricciones en el Uso de los Certificados	17
1.5.	Administración de la Política de Certificación	17
1.5.1.	Organización administradora del documento.....	17
1.5.2.	Persona de Contacto.....	17
1.5.3.	Persona que determina la idoneidad de la CPS.....	18
1.5.4.	Procedimiento de aprobación de la CPS	18
1.6.	Definiciones y abreviaturas	18
2.	Responsabilidades de publicación y repositorio.....	22
2.1.	Repositorios	22
2.2.	Publicación de la Información de certificación	22
2.3.	Tiempo o frecuencia de la Publicación.....	24
2.4.	Controles de Acceso a los Repositorios	24
3.	Identificación y Autenticación.....	26
3.1.	Nombres.....	26
3.1.1.	Tipos de Nombres	26
3.1.2.	Necesidad de que los nombres sean significativos	26
3.1.3.	Anonimato o Seudónimos de los Suscriptores.....	27
3.1.4.	Reglas de interpretación de diversas formas de nombre	27
3.1.5.	Unicidad de los nombres	27
3.1.6.	Reconocimiento, autenticación, y el rol de las marcas comerciales	27
3.2.	Validación de Identidad Inicial	27

3.2.1.	Acreditación	27
3.2.2.	Identidad	27
3.2.3.	Método para probar la posesión de la clave privada	28
3.2.4.	Información no verificada del suscriptor	28
3.2.5.	Validación de la autoridad	28
3.2.6.	Criterios para la interoperación	28
3.3.	Identificación y Autenticación para las solicitudes de cambio de claves	28
3.3.1.	Identificación y autenticación para la reasignación de clave rutinaria	28
3.3.2.	Identificación y autenticación para la reasignación de clave luego de la revocación ..	29
3.4.	Identificación y Autenticación para la Solicitud de Revocación	29
4.	Requerimientos operativos del ciclo de vida de los certificados	30
4.1.	Solicitud de certificados	30
4.1.1.	Quién puede presentar una solicitud de certificado	30
4.1.2.	Proceso de enrolamiento y responsabilidades	30
4.2.	Procesamiento de solicitud de certificado	30
4.2.1.	Realización de funciones de identificación y autenticación	30
4.2.2.	Aprobación o rechazo de las solicitudes de certificado	31
4.2.3.	Plazo para procesar las solicitudes de certificado	31
4.3.	Emisión de certificado	31
4.3.1.	Acciones de la CA durante la emisión del certificado	31
4.3.2.	Notificaciones al suscriptor de la emisión del certificado por parte de la CA	32
4.4.	Aceptación del certificado	32
4.4.1.	Conducta que constituye aceptación del certificado	32
4.4.2.	Publicación del certificado por la CA	32
4.4.3.	Notificación de la emisión del certificado a otras entidades por parte de la CA	32
4.5.	Uso del par de claves y del certificado	33
4.5.1.	Uso de la clave privada y certificado por el suscriptor	33
4.5.2.	Uso de la clave pública y certificado por el tercero aceptante	33
4.6.	Renovación de certificado	33
4.6.1.	Circunstancias para la renovación de certificado	34
4.6.2.	Quién puede solicitar la renovación	34
4.6.3.	Procesamiento de solicitudes de renovación de certificado	34
4.6.4.	Notificación al suscriptor de la emisión de un nuevo certificado	34
4.6.5.	Conducta que constituye aceptación del certificado de renovación	34
4.6.6.	Publicación del certificado renovado por la CA	34
4.6.7.	Notificación de la emisión del certificado por parte de la CA a otras entidades	35
4.7.	Cambio de claves del certificado	35

4.7.1.	Circunstancias para la reasignación de claves del certificado.....	35
4.7.2.	Quién puede solicitar la certificación de una nueva clave pública.....	35
4.7.3.	Procesamiento de solicitudes de reasignación de claves del certificado.....	35
4.7.4.	Notificación al suscriptor de la emisión de un nuevo certificado	35
4.7.5.	Conducta que constituye aceptación del certificado para claves reasignadas.....	35
4.7.6.	Publicación del certificado de clave reasignada por la CA.....	35
4.7.7.	Notificación de la emisión del certificado por parte de la CA a otras entidades.....	35
4.8.	Modificación del certificado.....	35
4.8.1.	Circunstancias para la modificación del certificado	36
4.8.2.	Quién puede solicitar modificación del certificado.....	36
4.8.3.	Procesamiento de solicitudes de modificación del certificado.....	36
4.8.4.	Notificación al suscriptor de la emisión de un nuevo certificado	36
4.8.5.	Conducta que constituye aceptación del certificado modificado	36
4.8.6.	Publicación del certificado modificado por la CA.....	36
4.8.7.	Notificación de la emisión del certificado por parte de la CA a otras entidades.....	36
4.9.	Revocación y suspensión de certificado	36
4.9.1.	Circunstancias para la revocación.....	36
4.9.2.	Quién puede solicitar la revocación	37
4.9.3.	Procedimiento para la solicitud de revocación.....	37
4.9.4.	Periodo de gracia de solicitud de revocación.....	38
4.9.5.	Tiempo dentro del cual la CA debe procesar la solicitud de revocación.....	38
4.9.6.	Requerimientos de comprobación de revocación por terceros aceptantes.....	38
4.9.7.	Frecuencia de emisión de CRL	38
4.9.8.	Latencia máxima de CRL	38
4.9.9.	Disponibilidad de comprobación en línea de revocación/estado	38
4.9.10.	Requerimientos de comprobación de revocación en línea.....	39
4.9.11.	Otras formas de publicidad de revocación disponibles.....	39
4.9.12.	Requerimientos especiales en relación con compromiso de claves	39
4.9.13.	Circunstancias para la suspensión.....	39
...3.	Suspensión de PSCA o ACPA.....	39
4.9.14.	Quién puede solicitar la suspensión	40
4.9.15.	Procedimiento para la solicitud de suspensión.....	40
4.9.16.	Límites del periodo de suspensión	40
4.10.	Servicios de estado de certificados.....	40
4.10.1.	Características operacionales	40
4.10.2.	Disponibilidad del servicio	40
4.10.3.	Características opcionales	40

4.11.	Fin de la suscripción	40
4.12.	Custodia (escrow) y recuperación de claves	42
4.12.1.	Políticas y prácticas de custodia y recuperación de claves	42
4.12.2.	Políticas y prácticas de encapsulamiento y recuperación de claves de sesión	42
5.	Gestión de las instalaciones y controles operacionales	43
5.1.	Controles físicos	43
5.1.1.	Localización del sitio y construcción	43
5.1.2.	Acceso físico	44
5.1.3.	Energía y aire acondicionado	44
5.1.4.	Exposición del agua	44
5.1.5.	Prevención y protección contra incendios	44
5.1.6.	Almacenamiento de medios	44
5.1.7.	Eliminación de residuos	45
5.1.8.	Respaldo fuera de las instalaciones (off-site)	45
5.2.	Controles de procedimiento	45
5.2.1.	Roles de confianza	45
5.2.2.	Número de personas requerido por tarea	46
5.2.3.	Identificación y autenticación para cada rol	46
5.2.4.	Roles que requieren separación de funciones	46
5.3.	Controles de personal	47
5.3.1.	Requerimientos de calificaciones, experiencia y habilitación	47
5.3.2.	Procedimiento de revisión de antecedentes	47
5.3.3.	Requerimientos de capacitación	48
5.3.4.	Requerimientos y frecuencia de re-capacitación	48
5.3.5.	Secuencia y frecuencia de rotación laboral	48
5.3.6.	Sanciones por acciones no autorizadas	48
5.3.7.	Requerimientos para contratista independiente	48
5.3.8.	Documentación proporcionada al personal	49
5.4.	Procedimiento de registro de auditoría	49
5.4.1.	Tipos de eventos registrados	49
5.4.2.	Frecuencia del procesamiento del registro (log)	50
5.4.3.	Periodo de retención para el registro (log) de auditoría	50
5.4.4.	Protección del registro (log) de auditoría	50
5.4.5.	Procedimiento de respaldo del registro (log) de auditoría	50
5.4.6.	Sistema de recopilación de archivo de auditoría (interno y externo)	50
5.4.7.	Notificación al sujeto causante del evento	51
5.4.8.	Evaluación de vulnerabilidades	51

5.5.	Archivo de registros.....	51
5.5.1.	Tipos de registros archivados	51
5.5.2.	Periodo de retención para el archivo	53
5.5.3.	Protección del archivo.....	53
5.5.4.	Procedimientos de respaldo del archivo.....	53
5.5.5.	Requerimientos para el sellado de tiempo (timestamp) de los registros	53
5.5.6.	Sistema de recopilación de archivo (interno o externo).....	53
5.5.7.	Procedimientos para obtener y verificar la información del archivo	54
5.6.	Cambio de clave	54
5.7.	Compromiso y recuperación de desastres (continuidad de operaciones)	54
5.7.1.	Procedimientos de manejo de incidentes y compromisos	54
5.7.2.	Corrupción de recursos de cómputo, datos y/o software	55
5.7.3.	Procedimientos ante el compromiso de clave privada de entidad.....	55
5.7.4.	Capacidades de continuidad de negocio después de un desastre	55
5.8.	Terminación de la CA o de la RA	55
5.9.	Procedimiento para el cambio de certificado de la ACPA	55
6.	Controles de Seguridad Técnica	56
6.1.	Generación e instalación del par de claves	56
6.1.1.	Generación del par de claves	56
...4.	Autoridad Certificadora Raíz Nacional.....	56
...5.	Autoridad Certificadora del Prestador Acreditado	56
6.1.2.	Entrega de la clave privada al suscriptor.....	56
6.1.3.	Entrega de la clave pública al emisor del certificado.....	57
6.1.4.	Entrega de la clave pública de la CA a los terceros aceptantes.....	57
6.1.5.	Tamaños de clave	57
6.1.6.	Generación y control de calidad de parámetros de clave pública	57
6.1.7.	Propósitos de uso de la clave (por campo Key Usage de certificado X.509 v3).....	57
6.2.	Protección de la clave privada y controles de ingeniería del módulo criptográfico	57
6.2.1.	Normas y controles para el módulo criptográfico.....	57
6.2.2.	Control multi-persona (m de un total de n) de la clave privada.....	57
6.2.3.	Custodia (escrow) de la clave privada	58
6.2.4.	Respaldo de la clave privada.....	58
6.2.5.	Archivo de la clave privada	58
6.2.6.	Transferencia de la clave privada desde/hacia un módulo criptográfico	58
6.2.7.	Almacenamiento de la clave privada en el módulo criptográfico	58
6.2.8.	Método de activación de la clave privada	59
6.2.9.	Método de desactivación de la clave privada.....	59

6.2.10.	Método de destrucción de la clave privada	59
6.2.11.	Clasificación del módulo criptográfico	59
6.3.	Otros aspectos de la gestión del par de claves	59
6.3.1.	Archivo de clave pública.....	59
6.3.2.	Periodos operacionales del certificado y periodos de uso del par de claves	60
6.4.	Datos de activación.....	60
6.4.1.	Generación e instalación de los datos de activación	61
6.4.2.	Protección de datos de activación	61
6.4.3.	Otros aspectos de los datos de activación	61
6.5.	Controles de seguridad computacional	61
6.5.1.	Requerimientos técnicos específicos de seguridad computacional.....	61
6.5.2.	Clasificación de la seguridad computacional.....	62
6.6.	Controles técnicos de ciclo de vida.....	62
6.6.1.	Controles de desarrollo de sistema.....	62
6.6.2.	Controles de gestión de la seguridad.....	62
6.6.3.	Controles de seguridad del ciclo de vida.....	62
6.7.	Controles de seguridad de la red.....	62
6.8.	Sellado de tiempo	63
7.	Perfiles de Certificado y CRL	64
7.1.	Perfil de certificado.....	64
7.1.1.	Número(s) de versión.....	64
7.1.2.	Extensiones del certificado	64
7.1.3.	Identificadores de objeto de algoritmos	64
7.1.4.	Formas de nombre.....	65
7.1.5.	Restricciones de nombres.....	65
7.1.6.	Identificadores de objeto de política de certificación.....	65
7.1.7.	Uso de la extensión “Policy Constraints”	66
7.1.8.	Sintaxis y semántica de calificadores de política	66
7.1.9.	Semántica de procesamiento para la extensión crítica “Certificate Policies”.....	66
7.1.10.	Perfiles	66
...6.	Perfil de certificado de la ACRN	66
...7.	Perfil de certificado de las ACPA.....	68
7.2.	Perfil de la CRL de la ACRN.....	70
7.2.1.	Número(s) de versión.....	70
7.2.2.	CRL y Extensiones de entradas CRL.....	70
7.3.	Perfil OCSP	70
7.3.1.	Número(s) de versión.....	70

7.3.2.	Extensiones OCSF	71
8.	Auditoría de cumplimiento y otras evaluaciones	72
8.1.	Frecuencia o circunstancias de evaluación	72
8.2.	Identidad/calificaciones del evaluador.....	72
8.3.	Relación del evaluador con la entidad evaluada	72
8.4.	Tópicos cubiertos por la evaluación	72
8.5.	Acciones a tomar como resultado de la deficiencia.....	73
8.6.	Comunicación de los resultados	73
9.	Otros aspectos comerciales y legales	74
9.1.	Tarifas	74
9.1.1.	Tarifas de emisión o renovación de certificados	74
9.1.2.	Tarifas de acceso a los certificados	74
9.1.3.	Tarifas de acceso a la información de estado o revocación.....	74
9.1.4.	Tarifas para otros servicios.....	74
9.1.5.	Política de reembolsos	74
9.2.	Responsabilidad financiera.....	74
9.2.1.	Cobertura de seguros.....	74
9.2.2.	Otros activos	74
9.2.3.	Garantía o cobertura de seguro para entidades finales.....	74
9.3.	Confidencialidad de la información de negocios.....	75
9.3.1.	Alcance de la información confidencial.....	75
9.3.2.	Información fuera del alcance de la información confidencial	75
9.3.3.	Responsabilidad de proteger la información confidencial	75
9.4.	Confidencialidad de la información personal	75
9.4.1.	Plan de privacidad.....	76
9.4.2.	Información personal	76
9.4.3.	Información pública	76
9.4.4.	Responsabilidad de proteger información privada.....	76
9.4.5.	Aviso y consentimiento de usar información privada	76
9.4.6.	Divulgación de conformidad con proceso judicial o administrativo.....	76
9.4.7.	Otras circunstancias de divulgación de información.....	77
9.5.	Derechos de propiedad intelectual.....	77
9.6.	Declaraciones y garantías	77
9.6.1.	Declaraciones y garantías de la CA	77
9.6.2.	Declaraciones y garantías de la RA	77
9.6.3.	Declaraciones y garantías del suscriptor	77
9.6.4.	Declaraciones y garantías del tercero aceptante.....	77

9.6.5.	Declaraciones y garantías de los demás participantes.....	78
9.7.	Renuncia de garantías	78
9.8.	Limitaciones de responsabilidad.....	78
9.9.	Indemnizaciones	78
9.10.	Vigencia y término	78
9.10.1.	Vigencia	78
9.10.2.	Término.....	78
9.10.3.	Efecto de término y sobrevivencia.....	79
9.11.	Avisos individuales y comunicaciones con los participantes.....	79
9.12.	Modificaciones	79
9.12.1.	Procedimiento para cambio de especificaciones.....	79
9.12.2.	Procedimiento de enmiendas	79
9.12.3.	Mecanismo y periodo de notificación.....	79
9.12.4.	Circunstancias en las que el OID debe ser cambiado.....	79
9.13.	Disposiciones de resolución de disputas	80
9.14.	Ley aplicable	80
9.15.	Conformidad con la ley aplicable.....	80
9.16.	Provisiones varias.....	80
9.16.1.	Acuerdo completo	80
9.16.2.	Asignación	80
9.16.3.	Divisibilidad.....	80
9.16.4.	Cumplimiento (honorarios de abogado y renuncia de derechos)	80
9.16.5.	Fuerza mayor	80
9.17.	Otras disposiciones.....	80
9.17.1.	Forma de interpretación y aplicación.....	80
9.17.2.	Obligaciones	81
...8.	Obligaciones de la UCE.....	81
...9.	Obligaciones de la ACRN.....	82
...10.	Obligaciones de los PSCA.....	83
9.17.3.	Obligaciones de las Autoridades de Registro de los Prestadores Acreditados	84
9.17.4.	Obligaciones de los Terceros Aceptantes	85
	Referencias Externas.....	87

1. Introducción

1.1. Descripción general

En el marco de la Infraestructura Nacional de Certificación Electrónica en Uruguay (PKI Uruguay, por sus siglas en inglés) funciona, como organismo acreditador y regulador, la Unidad de Certificación Electrónica (UCE).

La UCE cumple tres roles centrales en la operación de PKI Uruguay:

- promueve y aprueba las Políticas de Certificación que indican los perfiles de certificados electrónicos y aplicabilidad a diversos grupos de interés;
- acredita a Prestadores de Servicios de Certificación (PSC) a emitir certificados de acuerdo a estas Políticas; y,
- audita la actividad de los PSC.

De acuerdo a lo estipulado en la Ley 18.600, de 21 de setiembre de 2009[1], la operación de la Autoridad Certificadora Raíz Nacional (ACRN) es realizada por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). La ACRN es la raíz de la cadena de confianza. Su certificado es autofirmado y aceptado expresamente por los Terceros que establecen confianza en la PKI Uruguay.

La AGESIC, a través de la ACRN, habilita tecnológicamente la operación de los Prestadores de Servicios de Certificación Acreditados (PSCA) emitiendo certificados electrónicos para sus Autoridades Certificadoras (ACPA – Autoridad Certificadora del Prestador Acreditado). De esta forma, las ACPA pasan a ser parte de la cadena de confianza de la PKI Uruguay.

Los certificados emitidos por la ACRN y dirigidos a las ACPA se rigen por la presente Política de Certificación y por la Declaración de Prácticas de Certificación de la ACRN. Por lo tanto, las ACPA y los Terceros aceptantes de dichos certificados cuentan con el respaldo de PKI Uruguay para las operaciones de firma electrónica que correspondan.

La validez de la firma electrónica en Uruguay y la designación de los órganos competentes para su operación se encuentran declaradas en la Ley 18.600:

Artículo 1°. (Ámbito de aplicación).- Queda reconocida la admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica.

Los servicios de certificación electrónica deberán ajustarse a lo previsto en esta ley, su actividad no estará sujeta a autorización previa¹ y se realizará en régimen de libre competencia, sin que ello implique sustituir o modificar las normas que regulan las funciones que corresponde realizar a quienes están facultados legalmente para dar fe pública.

Las disposiciones de esta ley no alteran el Derecho preexistente respecto a la celebración, perfeccionamiento, validez y eficacia de los actos y negocios jurídicos.

Artículo 6°. (Efectos legales de la firma electrónica avanzada).- La firma electrónica avanzada tendrá idéntica validez y eficacia que la firma autógrafa consignada en documento público o en documento privado con firmas certificadas, siempre que esté debidamente autenticada por claves u otros procedimientos seguros que:

garanticen que la firma electrónica avanzada se corresponde con el certificado reconocido emitido por un prestador de servicios de certificación acreditado, que lo asocia con la identificación del signatario;

aseguren que la firma electrónica avanzada se corresponde con el documento respectivo y que el mismo no fue alterado ni pueda ser repudiado; y

garanticen que la firma electrónica avanzada ha sido creada usando medios que el signatario mantiene bajo su exclusivo control y durante la vigencia del certificado reconocido.

El documento electrónico suscripto con firma electrónica avanzada tendrá idéntico valor probatorio al documento público o al documento privado con firmas certificadas en soporte papel. El documento electrónico no hará fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador de servicios de certificación acreditado.

Artículo 14. (Competencia).- La Unidad de Certificación Electrónica deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de esta ley. A tales efectos tendrá las siguientes funciones y atribuciones:

De acreditación:

Recibir, tramitar y resolver las solicitudes de acreditación de los prestadores de servicios de certificación.

¹ Esto aplica a Autoridades Certificadoras de particulares. Los prestadores que operen bajo PKI Uruguay deberán estar previamente acreditados por la UCE.

Inscribir a los prestadores de servicios de certificación en el Registro de Prestadores de Servicios de Certificación Acreditados, que a tal efecto se crea en esta ley, una vez otorgada la acreditación.

Suspender o revocar la inscripción de los prestadores de servicios de certificación acreditados.

Mantener en el sitio web de la Unidad de Certificación Electrónica la información relativa al Registro de Prestadores de Servicios de Certificación Acreditados, tales como altas, bajas, sanciones y revocaciones.

De control:

Controlar la calidad y confiabilidad de los servicios brindados por los prestadores de servicios de certificación acreditados, así como los procedimientos de auditoría que se establezcan en la reglamentación.

Realizar auditorías a los prestadores de servicios de certificación acreditados, de conformidad con los criterios que la reglamentación establezca para verificar todos los aspectos relacionados con el ciclo de vida de los certificados reconocidos y de sus claves criptográficas.

Determinar las medidas que estime necesarias para proteger la confidencialidad de los titulares de certificados reconocidos.

Efectuar inspecciones y requerir en cualquier momento a los prestadores de servicios de certificación acreditados toda la información necesaria para garantizar el cumplimiento de la función en los términos definidos en esta ley y su reglamento.

De instrucción:

Recibir y evaluar reclamos de titulares de certificados reconocidos relativos a la prestación de servicios de certificación, sin perjuicio de la responsabilidad directa que el prestador de servicios de certificación acreditado tiene ante el titular.

De regulación:

Definir los estándares técnicos y operativos que deberán cumplir los prestadores de servicios de certificación acreditados, así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.

Fijar reglas y patrones industriales que aseguren la compatibilidad, interconexión e interoperabilidad, así como el correcto y seguro funcionamiento de los dispositivos de creación y verificación de firma, controlando su aplicación.

De sanción:

La Unidad de Certificación Electrónica podrá imponer al prestador de servicios de certificación acreditado que infringere total o parcialmente cualesquiera de las obligaciones derivadas de esta ley o de las normas que resulten aplicables al servicio que presta, las sanciones que se graduarán en atención a la gravedad o reiteración de la infracción, que se detallan a continuación:

Apercibimiento.

Multa entre 100.000 UI (cien mil unidades indexadas) y 4.000.000 UI (cuatro millones de unidades indexadas).

Suspensión hasta por un año de la acreditación.

Revocación de la acreditación.

Las sanciones podrán aplicarse independiente o conjuntamente, según resulte de las circunstancias del caso.

Las resoluciones que impongan sanciones pecuniarias de acuerdo a lo previsto en esta ley, constituyen título ejecutivo a todos sus efectos.

Artículo 15. (Autoridad Certificadora Raíz Nacional).- La Autoridad Certificadora Raíz Nacional es la primera autoridad de la cadena de certificación a la cual le compete emitir, distribuir, revocar y administrar los certificados de los prestadores de servicios de certificación acreditados.

Desígnase a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento como Autoridad Certificadora Raíz Nacional.



La presente Política de Certificación de la ACRN describe los certificados emitidos por la misma que habilitan la operación de las ACPA.

La presente Política de Certificación rige la actividad de la ACRN cumpliendo los requerimientos de “Certification Authority / Browser Forum Baseline Requirements (CABF Baseline Requirements)” [2] 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.

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 estipulados en el RFC 3647 [3]. Para preservar el esquema especificado en RFC 3647, las secciones que no aplican tienen la declaración “No es aplicable” o “No estipulado”.

Relación entre la Política de Certificación y otros documentos

Este documento contiene la Política de Certificación de la Unidad de Certificación Electrónica (UCE). Una Política de Certificación es un conjunto de principios y reglas relativas a la emisión y gestión de certificados electrónicos, con soporte de claves públicas, que pueden utilizarse en diferentes servicios, como la autenticación de la identidad, la integridad y la autenticidad documental o el secreto de los datos, documentos y transmisiones.

La Política de Certificación establece las reglas mínimas que se deben cumplir por parte de los Prestadores de Servicios de Certificación Acreditados (PSCA) y los terceros aceptantes de certificados.

Por otra parte, todo Prestador de Servicios de Certificación debe disponer de una Declaración de Prácticas de Certificación con los procedimientos que aplica en la prestación de sus servicios, en cumplimiento con lo establecido en la Ley No 18.600, indicando el grado de aplicación de los requisitos establecidos por las Políticas de Certificación que gestiona detallando sus prácticas profesionales en relación con la provisión de los servicios de certificación.

Esta documentación se relaciona con la documentación auxiliar, entre la que se deben encontrar los instrumentos jurídicos reguladores de la prestación de servicios (documentación jurídica auxiliar), documentación de seguridad, documentación de operación y documentación de archivo.

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

Nombre: Política de Certificación de la ACRN

Versión: 2.2

Fecha de elaboración: 05/10/2011

Fecha de última actualización: 18/03/2024

OID: 2.16.858.10000157.66565.1

Sitio web de publicación: <https://www.gub.uy/unidad-certificacion-electronica/comunicacion/publicaciones/politicas-certificacion-autoridades-certificadoras-servicios-confianza>

1.3. Participantes de la INCE

1.3.1. Autoridad Certificadora

El rol de Autoridad de Certificación incluye las funciones relativas a la gestión de certificados electrónicos que habiliten o inhabiliten tecnológicamente la operación de los Prestadores de Servicios de Certificación Acreditados, según lo dispuesto por la presente Política de Certificación y la normativa legal vigente. El rol de Autoridad de Certificación para la ACRN es cumplido por la AGESIC según lo estipulado por la Ley 18.600. La Autoridad de Certificación responde a las solicitudes del Suscriptor de los certificados a través de su Autoridad de Registro (ver 1.3.3 – Autoridad de Registro).

Como autoridad de certificación, la ACRN desempeña las siguientes funciones:

- a) Emitir, Renovar y Revocar el certificado público de la ACRN;
- b) A solicitud de la UCE, Emitir, Renovar y Revocar certificados que habilitan la operación de los PSCA;
- c) Publicar y mantener actualizada la Lista de Certificados Revocados (CRL, por sus siglas en inglés) para todos los certificados emitidos que apliquen a la presente Política;
- d) Publicar documentación de la ACRN y aplicable a ella, como la presente Política de Certificación, la Declaración de Prácticas de Certificación de la ACRN y el Acuerdo con los PSC;
- e) Publicar los certificados emitidos a los PSCA.

La ACRN asume las responsabilidades y obligaciones estipuladas en el punto 9.17.2.2.

1.3.2. Autoridad de Registro

La Autoridad de Registro es la dependencia que atiende y procesa las solicitudes de emisión, renovación o revocación de certificados de parte del Suscriptor (punto 15).

En el caso de la ACRN, las funciones de Autoridad de Registro las realizará AGESIC.

Las responsabilidades y acciones realizadas por la Autoridad de Registro se encuentran descriptas en la sección 84 de la presente Política de Certificación.

1.3.3. Suscriptores

Los suscriptores de los certificados emitidos por la ACRN son los PSCA.

...1. Prestadores de Servicios de Certificación Acreditados

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.

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.

Los PSCA asumen las responsabilidades y obligaciones estipuladas en el punto **¡Error! Marcador no definido..**

1.3.4. Terceros Aceptantes

Los Terceros aceptantes son las entidades o personas que confían en los certificados emitidos por la ACRN a los PSCA bajo la presente Política. Los Terceros aceptantes utilizan estos certificados para validar la cadena de confianza de la PKI.

Los terceros aceptantes deben asumir las responsabilidades y obligaciones estipuladas en el punto 9.17.2.5.

1.3.5. Otros participantes

...2. Unidad Reguladora

El rol de Ente regulador incluye la totalidad de funciones relativas a la definición de las normas que regulan el funcionamiento de los diferentes actores de la Infraestructura Nacional de Certificación Electrónica. De acuerdo a la Ley 18.600 ese rol es desempeñado por la UCE.

Como unidad reguladora, la UCE desempeña las siguientes funciones:

- a) Definir y aprobar las Políticas de Certificación que definen los perfiles de certificados de la PKI Uruguay;
- b) Desarrollar el proceso de acreditación de Prestadores, autorizando o denegando la operación de los mismos dentro de la PKI Uruguay;
- c) Solicitar a la Unidad Nacional de Asignación de OID (UNAOID), en su rol de Administrador de la rama de OIDs de Uruguay, un OID para cada Política de Certificación aprobada;
- d) Publicar y mantener actualizada la Lista de Prestadores de Servicios de Certificación Acreditados y Suspendidos, incluyendo la información pública de contacto de cada uno de ellos y las Políticas de Certificación para las cuales están acreditados a emitir certificados;
- e) Realizar auditorías periódicas a los PSCA para verificar el cumplimiento con las normativas legales vigentes y las Políticas de Certificación para las cuales emiten certificados

Las obligaciones asumidas por la UCE se estipulan en el punto **¡Error! Marcador no definido..**

1.4. Uso de los certificados

1.4.1. Usos Permitidos de los Certificados

Los certificados emitidos por la ACRN bajo la presente Política de Certificación pueden ser utilizados por los PSCA con el único propósito de validar la cadena de confianza de la PKI, firmar los certificados emitidos a sus suscriptores finales y firmar las Listas de Revocación de Certificados correspondientes.

1.4.2. Restricciones en el Uso de los Certificados

Los certificados no pueden ser utilizados con otro fin a los estipulados en el punto 1.4.1. La utilización de la llave privada asociada al certificado para otro fin es considerada causal de revocación del mismo (ver 4.9.1).

1.5. Administración de la Política de Certificación

1.5.1. Organización administradora del documento

La administración de la presente Política de Certificación 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 0065 opción 5

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.

1.5.4. Procedimiento de aprobación de la CPS

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.

1.6. 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 [1]. No obstante, las siguientes definiciones y abreviaturas son utilizadas a lo largo del presente documento, y por lo tanto, son citadas también aquí.

Autoridad Certificadora Raíz Nacional (ACRN): conjunto de sistemas informáticos, personal, políticas y procedimientos que, en la estructura de PKI Uruguay por herencia, constituyen la raíz de confianza. Permite certificar a otras entidades encargadas de emitir certificados dentro de PKI Uruguay. Ver punto 1.3.1.

Prestador de Servicios de Certificación Acreditado (PSCA): entidad acreditada ante la UCE y responsable de la operación de una Autoridad de Certificación de PKI Uruguay. Ver punto 1.3.3.1

Autoridad Certificadora del Prestador Acreditado (ACPA): suscriptor de los certificados emitidos por la ACRN que, durante su operativa, emite certificados a usuarios finales bajo las políticas de certificación que le fueron asignadas.

Terceros aceptantes: en el contexto de PKI Uruguay, usuarios que validan y confían en certificados emitidos por una Autoridad de Certificación de la PKI, sea la ACRN o una de las ACPA. Ver punto 1.3.4.

Política de Certificación (CP – Certificate Policy): conjunto de políticas que indican la aplicabilidad de un certificado a una comunidad particular y/o clase de solicitud con

requerimientos comunes de seguridad, y además definen los requisitos que cualquier prestador debe respetar para trabajar con ese tipo de certificado. En el contexto de PKI Uruguay estas políticas son promovidas, aprobadas y mantenidas por la UCE.

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

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

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.

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.

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. Para la presente política los suscriptores serán los PSCA. Ver 1.3.3.

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 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 1.3.2.

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.

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:

4. Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;
5. 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,
6. 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.

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.

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

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

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

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

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

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

2. Responsabilidades de publicación y repositorio

2.1. Repositorios

La UCE dispone como repositorio público de información el siguiente sitio web:

- www.uce.gub.uy

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

- <https://www.gub.uy/unidad-certificacion-electronica/comunicacion/publicaciones/politicas-certificacion-autoridades-certificadoras-servicios-confianza>

La ACRN deberá 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.

2.2. Publicación de la Información de certificación

Para esta política de certificación es obligación de la UCE el mantenimiento de un repositorio público de información, a través de un sitio web, que contenga la siguiente información:

- a) Esta Política de Certificación (versión vigente y anteriores);
- b) Todas las políticas de certificación que regulan la PKI Uruguay (versiones vigentes y anteriores);
- c) Los requerimientos para la acreditación de un PSC;
- d) Las resoluciones mediante las que se acredita, suspende, renueva, revoca o deniega la acreditación a los PSC, con las razones pertinentes en el caso de suspensiones o revocaciones;
- e) La lista de OIDs de políticas de certificación de la UCE bajo las que emiten certificados las ACPA, detallando qué OIDS está autorizada a utilizar en los certificados emitidos cada ACPA;

- f) La lista de OIDs de la Declaración de Prácticas de Certificación de los PSCA;
- g) Las listas de Certificados Revocados (CRL) de los PSCA, incluyendo la de la ACRN;
- h) Información relevante de los informes de auditoría de la que fue objeto la UCE, la ACRN y los PSCA;
- i) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto de la UCE;
- j) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto de la ACRN;
- k) Identificación, domicilios, números telefónicos y direcciones de correo electrónico de los contactos designados por los PSCA para la atención a suscriptores finales y Terceros aceptantes;
- l) Identificación, domicilio, números telefónico y dirección de correo electrónico de los PSC cuya acreditación haya sido revocada o expirado;
- m) Leyes, Decretos y demás documentos regulatorios que afecten a la PKI Uruguay.

Para esta política de certificación es obligación de la ACRN el mantenimiento de un repositorio público de información, a través de un sitio web, que contenga la siguiente información:

- a) Todas las políticas de certificación (versiones vigentes y anteriores) que utilice la ACRN para la emisión de certificados, incluyendo esta;
- b) La Declaración de Prácticas de Certificación de la ACRN (versión vigente y anteriores);
- c) El certificado autofirmado de la ACRN;
- d) Los certificados emitidos por la ACRN a las ACPA;
- e) La Lista de Certificados Revocados (CRL) de la ACRN;
- f) Referencia al sitio de publicación de información de la UCE;
- g) Identificación, domicilio, números telefónicos y direcciones de correo electrónico de contacto de la ACRN.

La publicación o actualización de la información contenida en el repositorio público deberá contar con la verificación y aprobación de la UCE o de la ACRN según corresponda.

La UCE publicará en su sitio web las modificaciones aprobadas a la presente Política de Certificación, indicando en cada caso las secciones y/o textos reemplazados junto con la publicación de la nueva versión. Además, publicará un vínculo a los mismos en el Diario Oficial durante un (1) día hábil.

Lo anteriormente estipulado también aplica al Acuerdo con Suscriptores de Certificados. Los PSCA serán notificados directamente ante cualquier cambio en estos términos o en la presente Política de Certificación.

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 disponible de nuevo en un periodo establecido en 48 horas.

La ACRN deberá garantizar niveles de servicio análogos para su servicio de publicación de información.

2.3. Tiempo o frecuencia de la Publicación

La información sobre políticas de certificación, acuerdos de privacidad y otros documentos relacionados será actualizada 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.

La información relativa al estado de la acreditación de los PSC será actualizada con un máximo de un (1) día hábil desde que se produzcan cambios.

La Lista de Certificados Revocados (CRL) de la ACRN deberá ser actualizada cuando ocurra al menos uno de los siguientes hechos:

- a) se produzca la revocación de un certificado;
- b) transcurran tres (3) meses desde la última emisión de la CRL

Se realizan revisiones anuales al presente documento.

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.

3. Identificación y Autenticación

3.1. Nombres

3.1.1. Tipos de Nombres

Para el nombre de la ACPA se deberá utilizar el campo “Subject” del certificado emitido por la ACRN (ver **¡Error! Marcador no definido. ¡Error! No se encuentra el origen de la referencia.**). El formato para indicar el nombre de la ACPA deberá ser X.500 (Distinguished Name).

Dicho formato, se aplicará de la siguiente forma:

Country: País del Prestador (UY)

Organization: Nombre legal o de fantasía del prestador.

Common Name: Nombre de la Autoridad Certificadora del Prestador.

Eventualmente, podrá elegir el orden inverso de modo que quede CN,O,C.

Por mayor detalle acerca de la nominación y formatos de los nombres, referir al Punto 7 – **¡Error! No se encuentra el origen de la referencia.**

A modo de ejemplo, el “Prestador ABC” podrá elegir su nombre distinguido de la siguiente manera:

C=UY

O=ABC

CN=Autoridad Certificadora de ABC

Pudiendo el orden de los elementos del campo “Sujeto” ser el inverso y conteniendo otros elementos tal y como se describe en el punto 7.

3.1.2. Necesidad de que los nombres sean significativos

El nombre de la ACPA debe ser elegido por el PSCA.

El nombre elegido debe ser distintivo y estar asociado semánticamente al nombre legal del PSCA. Por ejemplo, si el nombre legal del PSCA fuera “Prestador ABC”, un nombre apropiado sería “Autoridad Certificadora del Prestador ABC”.

Los nombres elegidos deben ser únicos en el ámbito de la ACRN, de forma de identificar inequívocamente a cada PSCA.

En caso de que el PSCA opere más de una ACPA, los nombres para cada ACPA deben ser distintos.

La Autoridad de Registro de la ACRN asignará a la ACPA el nombre que figure en la resolución de acreditación correspondiente. Es responsabilidad de la UCE la aprobación de dicho nombre durante la acreditación.

3.1.3. Anonimato o Seudónimos de los Suscriptores

No se permite el anonimato de los suscriptores (ACPA). Sin embargo, se permite el uso de un nombre de fantasía como es estipulado en el punto 3.1.1.

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.

3.1.5. Unicidad de los nombres

Las ACRN deben forzar la unicidad de los nombres en los certificados emitidos bajo la presente Política.

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. A no ser que se especifique en otro lugar, esta CP no requiere que se verifique el derecho de un solicitante a utilizar una marca comercial.

3.2. Validación de Identidad Inicial

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

3.2.1. Acreditación

Previo al proceso de registro, el PSC debe acreditarse ante la UCE para poder operar en el contexto de PKI Uruguay. Los requerimientos para la acreditación se encuentran en el Procedimiento para la acreditación como Prestador de Servicios de Certificación de PKI Uruguay, disponible en <https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados>.

El PSCA debe demostrar ante la Autoridad de Registro de la ACRN la acreditación vigente ante la UCE.

3.2.2. Identidad

La persona física designada por el PSCA para tramitar la emisión de un certificado, además de presentar la resolución de acreditación ante la UCE, deberá demostrar ante la

Autoridad de Registro de la ACRN su identidad, presentando el documento de identificación correspondiente.

La ACRN deberá verificar que dichos datos además coincidan con los establecidos en la resolución de acreditación, la cual contendrá el nombre y número de documento de las personas autorizadas a solicitar el certificado.

3.2.3. Método para probar la posesión de la clave privada

Para la emisión del certificado bajo la presente Política de Certificación, la ACRN debe validar que la llave privada correspondiente a la llave pública del CSR (Certificate Signing Request), emitido por una ACPA, este en posesión del PSCA y sea la misma utilizada para firmarlo. Para garantizar esto, un funcionario designado por la UCE y uno designado por la ACRN deberán estar presentes en el acto de generación de las llaves de la ACPA y firmar su conformidad con el proceso (ver 4.1 y 6.1.2). En ningún caso el PSCA se encuentra autorizado a compartir la llave privada de su/s ACPA con la ACRN (ver 4.1 Solicitud de Certificado).

Para el caso en que un PSCA opere más de una ACPA, los certificados y las llaves privadas asociadas deben ser únicos por ACPA.

3.2.4. Información no verificada del suscriptor

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

3.2.5. Validación de la autoridad

No aplica.

3.2.6. Criterios para la interoperación

No aplica.

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

No está permitido el cambio de claves de las ACPA ni de la ACRN como proceso independiente. Puede realizarse un cambio de clave en el marco de los procesos de renovación o revocación y re-emisión de certificados.

3.3.1. Identificación y autenticación para la reasignación de clave rutinaria

No aplica.

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

No aplica.

3.4. Identificación y Autenticación para la Solicitud de Revocación

La Autoridad de Registro de la ACRN debe validar la identidad del solicitante previamente a la solicitud de revocación del certificado emitido a una ACPA del PSCA. Para ello, el solicitante deberá estar habilitado por la UCE para solicitar la revocación y deberá identificarse oportunamente al igual que en el punto 3.1.2.2.

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.

4. Requerimientos operativos del ciclo de vida de los certificados

Los siguientes requerimientos están dirigidos a la ACRN, en su rol de Autoridad de Certificación Raíz, y a los PSCA en su rol de Suscriptores de los certificados emitidos bajo la presente Política. El objetivo es permitir una gestión segura del Ciclo de Vida de los Certificados emitidos por la ACRN.

4.1. Solicitud de certificados

El PSCA solicita la emisión de un certificado ante la Autoridad de Registro de la ACRN, presentando la información requerida (ver 3.1 - Registro Inicial).

La Autoridad de Registro de la ACRN debe validar la información presentada, y la generación de las claves debe satisfacer los requerimientos de seguridad y controles estipulados en la Declaración de Prácticas de Certificación de la ACRN.

4.1.1. Quién puede presentar una solicitud de certificado

El PSCA podrá solicitar la emisión de los certificados ante la Autoridad de Registro de la ACRN. Dichos certificados serán emitidos bajo la presente Política de Certificación.

4.1.2. Proceso de enrolamiento y responsabilidades

El PSC deberá demostrar ante la ACRN una resolución de acreditación vigente ante la UCE para cada emisión de certificado que solicite.

Los certificados emitidos por la ACRN bajo la presente Política de Certificación habilitan tecnológicamente la operación de las ACPA como Autoridades de Certificación subordinadas de la ACRN dentro de la cadena de confianza de la PKI Uruguay. Las ACPA del PSCA, en caso de que operara más de una, se ubican al mismo nivel dentro de la cadena de confianza. No se permite en el contexto de PKI Uruguay la existencia de una ACPA subordinada a otra ACPA.

4.2. Procesamiento de solicitud de certificado

4.2.1. Realización de funciones de identificación y autenticación

Las ACRN deberán mantener los sistemas y procesos para autenticar satisfactoriamente a los solicitantes de acuerdo a lo establecido en 3.2.

4.2.2. Aprobación o rechazo de las solicitudes de certificado

La ACRN deberá validar el CSR emitido por el PSCA. Para dicha verificación, la ACRN debe comprobar que:

- a) la información contenida en el CSR es consistente con la información de acreditación ante la UCE;
- b) el CSR se encuentra firmado con la clave privada correspondiente a la clave pública en él contenida;
- c) existen pruebas fehacientes de que la clave privada con que se firmó el CSR está en exclusivo poder del PSCA, y que además ésta fue generada de acuerdo a los requerimientos estipulados en la sección 6.1.2 de la presente Política. Para este punto es suficiente una declaración de conformidad por parte del funcionario designado para presenciar la generación, o por los auditores designados para tal tarea;
- d) el CSR contiene los campos requeridos por la presente Política de Certificación, de acuerdo a lo estipulado en el Punto 7 – Perfiles de Certificados y Listas de Certificados Revocados.

Si la verificación es satisfactoria, se da inicio a la Emisión de Certificado.

Una vez que la Autoridad de Registro del ACRN registró la solicitud de certificado – según se especifica en la sección 4.1.2 - y se validó el CSR emitido por el PSCA la ACRN autoriza y da inicio a la emisión del certificado.

En ningún momento, durante el procesamiento de la solicitud de certificado, la ACRN puede acceder a la clave privada del Suscriptor.

4.2.3. Plazo para procesar las solicitudes de certificado

Luego de que un Prestador de Servicios de Certificación se Acredite ante la UCE y solicite un certificado para su ACPA se dispondrán de 10 días hábiles para la emisión del mismo.

4.3. Emisión de certificado

4.3.1. Acciones de la CA durante la emisión del certificado

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

La ACRN 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 **¡Error! Marcador no definido.** de esta Política.

El período de validez del certificado emitido deberá ser el período comprendido entre la fecha de emisión y la fecha de expiración del certificado de la ACRN, excepto que sea revocado con anterioridad dicha fecha. Sin perjuicio de lo establecido, en caso de que la evolución tecnológica pueda generar riesgo criptográfico, obsolescencia de sistemas o problemáticas afines, la UCE podrá determinar por vía regulatoria la obligatoriedad de efectuar las adecuaciones que entienda pertinentes.

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

La ACRN deberá informar al PSCA de la emisión del Certificado de una manera conveniente y apropiada basado en la información suministrada en el proceso de acreditación.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye aceptación del certificado

El PSCA procede a la validación del mismo. Verifica que la información contenida en el certificado y la firma de la ACRN sean correctas.

En caso de que el PSCA acepte el certificado, deberá entregar a la ACRN el Acuerdo de Suscriptores firmado por su representante legal en un plazo no menor a veinticuatro horas (24) y proceder a la instalación del certificado en su ACPA en presencia del funcionario de la ACRN que lo entregó. En caso contrario se deberá proceder a la modificación del certificado, o a la revocación del mismo dependiendo de la magnitud de la discordancia.

4.4.2. Publicación del certificado por la CA

La ACRN deberá publicar el certificado emitido, junto a la información de contacto del PSCA, en su repositorio público de información. A partir de dicha instancia se considera válida la operación de la ACPA.

Se publicará el certificado emitido, junto a la información de contacto del PSCA, en el repositorio público de información de la UCE, y se publicará al menos un (1) día en el Diario Oficial una referencia a dicha información.

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

La ACRN notificará a la UCE de la emisión del certificado.

4.5. Uso del par de claves y del certificado

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

El PSCA debe utilizar la clave privada asociada al certificado emitido por la ACRN únicamente para firmar los certificados emitidos por su ACPA y la Lista de Revocación de Certificados bajo las Políticas de Certificación para las que fue acreditado por la UCE.

En ningún caso se encuentra autorizado el uso de la llave privada asociada al certificado para firmar otros documentos, cifrar información o realizar funciones de autenticación. La utilización de dicha llave para otro fin puede ser causal de revocación del certificado y/o suspensión de la acreditación del PSC.

El PSCA deberá mantener el certificado público emitido por la ACRN bajo la presente Política de Certificación en un repositorio público de información.

El PSCA deberá tomar las medidas de seguridad especificadas en la presente Política y en la Declaración de Prácticas de Certificación de la ACRN para la protección de la llave privada.

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 **¡Error! Marcador no definido.**);
- 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.

4.6.1. Circunstancias para la renovación de certificado

La Renovación del Certificado es el proceso en el que la ACRN emite un nuevo certificado a la ACPA para que continúe sus operaciones una vez vencido el certificado anterior. No está permitido mantener el mismo par de llaves para diferentes certificados, por lo que el PSCA debe generar un par de llaves nuevo, con los requerimientos de seguridad definidos para la emisión de certificados (Ver 4.3).

Una ACPA de PSCA no puede emitir certificados que expiren en una fecha posterior a la de expiración de su propio certificado, por lo cual un PSCA podrá solicitar la emisión de un nuevo certificado con una antelación máxima de un (1) año antes de que expire el que posee. Luego de la emisión del nuevo certificado y hasta la expiración del anterior, el PSCA podrá operar con los dos certificados. El certificado anterior podrá ser utilizado únicamente para firmar la Lista de Revocación de Certificados correspondiente y validar la cadena de confianza de PKI Uruguay. El nuevo certificado podrá ser utilizado para las operaciones de emisión de nuevos certificados y firma de la nueva Lista de Revocación de Certificados

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 y deberá aplicarse el procedimiento para modificación del certificado (Ver 4.8).

4.6.2. Quién puede solicitar la renovación

La solicitud de renovación debe ser realizada por el PSCA.

4.6.3. Procesamiento de solicitudes de renovación de certificado

Para la renovación del certificado, el PSCA debe presentar una constancia de acreditación emitida por la UCE con vigencia a la fecha en que se realice la solicitud. La solicitud debe ser presentada a la Autoridad de Registro de la ACRN, la cual deberá validarla en conformidad con lo establecido en el punto 3.2.

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

La ACRN deberá informar al PSCA de la renovación del Certificado de una manera conveniente y apropiada basado en la información suministrada en el proceso de acreditación.

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. Cambio de claves del certificado

El Cambio de Clave del certificado no es un procedimiento permitido. Debe en su lugar aplicarse los procedimientos de Revocación y Emisión de Certificado en el mencionado orden o el de Renovación si es que la fecha de expiración es próxima.

4.7.1. Circunstancias para la reasignación de claves del certificado

No aplica.

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

No aplica.

4.7.3. Procesamiento de solicitudes de reasignación de claves del certificado

No aplica.

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

No aplica.

4.7.5. Conducta que constituye aceptación del certificado para claves reasignadas

No aplica.

4.7.6. Publicación del certificado de clave reasignada por la CA

No aplica.

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

No aplica.

4.8. 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.

4.8.1. Circunstancias para la modificación del certificado

La Modificación del Certificado es permitida únicamente en el caso en que la ACRN emitiera un certificado con información errónea o imprecisa debido a un error interno y no a la información provista por el PSCA, y debe ser solicitada por el PSCA previamente a la aceptación formal del certificado. En cualquier otro caso, deben aplicarse los procedimientos de Revocación y Emisión de Certificado en el mencionado orden.

4.8.2. Quién puede solicitar modificación del certificado

La solicitud de modificación debe ser realizada por el PSCA previo a la aceptación formal del certificado.

4.8.3. Procesamiento de solicitudes de modificación del certificado

Se aplicarán los mismos procedimientos que en la emisión de un certificado nuevo, como se estipula en 4.2

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

Se aplicarán los mismos procedimientos que en la emisión de un certificado, como se estipula en 4.3.2

4.8.5. Conducta que constituye aceptación del certificado modificado

Se aplicarán los mismos procedimientos que en la emisión de un certificado, como se estipula en 4.4.1

4.8.6. Publicación del certificado modificado por la CA

Se aplicarán los mismos procedimientos que en la emisión de un certificado, como se estipula en 4.4.2

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

Se aplicarán los mismos procedimientos que en la emisión de un certificado, como se estipula en 4.4.3

4.9. Revocación y suspensión de certificado

4.9.1. Circunstancias para la revocación

La Revocación del Certificado es un procedimiento que anula definitivamente la validez de un certificado emitido por la ACRN, independientemente de su fecha de expiración.

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

En caso de que el PSC pretenda continuar prestando servicios de certificación dentro de PKI Uruguay luego de la revocación, deberá acreditarse nuevamente ante la UCE.

Las causales para la revocación del certificado son las siguientes:

- cuando existan evidencias de que la clave privada de la ACPA se encuentre comprometida, en un medio de almacenamiento comprometido o con riesgo cierto de estarlo;
- si se constata un incumplimiento grave de las Políticas de Certificación para las cuales emite certificados y/o las Prácticas de Certificación por las cuales se debe regir;
- si se constata que el PSCA está haciendo usos del certificado no permitidos por la presente Política de Certificación o las Políticas de Certificación según las cuales emite certificados;
- si es revocada la acreditación del PSC por resolución de la UCE;
- si el PSCA desea finalizar las operaciones de alguna de sus ACPA;
- por resolución de una autoridad judicial competente;
- otras causales especificadas en regulaciones emitidas por la UCE.

4.9.2. Quién puede solicitar la revocación

La UCE será quien disponga la revocación de un certificado, por resolución propia, a solicitud de un PSCA, a solicitud de la ACRN o a solicitud de una autoridad judicial competente.

4.9.3. Procedimiento para la solicitud de revocación

En el caso de que el PSCA realice la solicitud de revocación, debe emitir una constancia escrita y aprobada por su representante legal para informar a la UCE. De ser aceptada y debidamente autenticada (ver 3.4), la UCE dispondrá la revocación. La UCE autoriza a la Autoridad de Registro de la ACRN para atender solicitudes de revocación de PSCA en escenarios de urgencia por motivos de seguridad, informando luego a la misma.

El PSCA, en caso de continuar sus operaciones, debe mantener publicada la CRL con todos los certificados revocados, y mantener disponible la base de datos OCSP si contara con una. Además, deberá realizar nuevamente el proceso de acreditación ante la UCE.

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

La ACRN tiene un período máximo de un (1) día a partir de la resolución de la UCE para revocar el certificado y publicar la CRL actualizada en el repositorio público de información.

El PSCA tiene un plazo máximo de un (1) día a partir de la revocación efectiva de su certificado para revocar todos los certificados emitidos con él y publicar una CRL o actualizar las bases de datos OCSP. Finalizado este procedimiento, el PSCA procederá a la destrucción de su clave privada mediante un mecanismo que impida su reconstrucción, para evitar compromisos futuros de esa clave. Este proceso deberá ser presenciado por un representante de la ACRN.

4.9.6. Requerimientos de comprobación de revocación por terceros aceptantes

Para la validación de un certificado (ver sección **¡Error! Marcador no definido.**), 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.

4.9.7. Frecuencia de emisión de CRL

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 plazos para emitir una CRL luego de la revocación de un certificado final se especifican en la política de certificación de dicho certificado.

4.9.8. Latencia máxima de CRL

Un pedido de revocación recibido 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

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

Ni la ACRN ni la UCE se responsabilizan por ningún tipo de incidente que derive de una falta de verificación de la CRL de la ACPA en el momento de validación de un certificado por parte de los Terceros aceptantes.

La ACRN deberá garantizar alta disponibilidad de la información, a excepción de los períodos planificados de mantenimiento.

La ACRN publicará esta información en <https://www.gub.uy/unidad-certificacion-electronica/comunicacion/publicaciones/declaracion-practicas-certificacion>, y deberá especificar la URL concreta de publicación de estos servicios en su CPS.

4.9.10. Requerimientos de comprobación de revocación en línea

Los terceros aceptantes deberán confirmar la información de revocación como es estipulado en 4.9.6.

4.9.11. Otras formas de publicidad de revocación disponibles

No estipulado.

4.9.12. Requerimientos especiales en relación con compromiso de claves

La ACRN y las ACPAs deberá usar métodos razonables para informar a sus suscriptores que su clave privada ha sido comprometida. Esto incluye casos donde nuevas vulnerabilidades fueron descubiertas o donde la ACRN o las ACPAs 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 ACRN o las ACPAs deberán 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

La suspensión de certificados emitidos por la ACRN no es un proceso permitido.

...3. Suspensión de PSCA o ACPA

La suspensión de un PSCA o de una ACPA es un proceso mediante el cual se prohíbe que ésta emita certificados electrónicos por el tiempo que dure la suspensión.

Una suspensión puede dar lugar a una revocación del certificado de la ACPA, si la UCE lo considera pertinente.

Las causales para la suspensión son las siguientes:

- a) si se constata que la información contenida en el certificado es errónea o se encuentra desactualizada;
- b) si se determina que existieron errores en los procedimientos operativos asociados a la emisión del certificado;
- c) si se realizan cambios significativos en la presente Política de Certificación;
- d) por resolución de una autoridad judicial competente;
- e) otras causales especificadas en regulaciones emitidas por la UCE.

4.9.14. Quién puede solicitar la suspensión

La suspensión podrá ser solicitada por la ACRN, por una autoridad judicial competente o por resolución de la UCE.

4.9.15. Procedimiento para la solicitud de suspensión

La UCE será quien disponga la suspensión de un PSCA o ACPA, por resolución propia a solicitud de un PSCA, a solicitud de la ACRN o a solicitud de una autoridad judicial competente.

4.9.16. Límites del periodo de suspensión

No estipulado.

4.10. Servicios de estado de certificados

4.10.1. Características operacionales

Los PSCA deberán 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.

4.10.2. Disponibilidad del servicio

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

4.10.3. Características opcionales

No estipulado.

4.11. Fin de la suscripción

La finalización de la suscripción refiere a las situaciones en las que el certificado alcance su fecha de expiración, en que la ACRN finalice sus servicios o en que la ACPA finalice sus servicios.

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

La ACRN deberá especificar en su Declaración de Prácticas de Certificación el procedimiento para el eventual cese de sus actividades.

En la eventualidad de que un PSCA finalice sus servicios o finalice los servicios de una de sus ACPA:

- a) el PSCA deberá publicar la fecha de suspensión de las actividades de la ACPA con sesenta (60) días de antelación en su Sitio Oficial y una referencia a dicha información en el Diario Oficial durante un (1) día hábil;
- b) el PSCA deberá notificar a los suscriptores de los certificados emitidos por la ACPA en un plazo menor a quince (15) días luego de anunciada su suspensión en su Sitio Oficial y en el Diario Oficial;
- c) la UCE procederá a la suspensión de la ACPA del PSCA, inhabilitándola a emitir y/o renovar certificados;
- d) luego de expirados todos los certificados de suscriptores de la ACPA, el PSCA deberá proceder a la destrucción de la clave privada de la ACPA mediante un mecanismo que impida su reconstrucción, según fue especificado en su Declaración de Prácticas de Certificación;
- e) la UCE publicará en su Sitio Oficial, y una referencia en el Diario Oficial, el cese total de actividades de la ACPA del PSCA;
- f) el certificado de la ACPA, el directorio de certificados emitidos por ella y la última lista de revocación emitida deberán ser transferidos a la UCE;
- g) la UCE publicará en su Sitio Oficial, y una referencia en el Diario Oficial, el enlace al sitio donde se encuentra la lista de revocación y el certificado de la ACPA que finalizó sus operaciones.

Luego de la suspensión de la ACPA del PSCA (numeral c), esta no podrá emitir ningún certificado, pero deberá continuar dando soporte a las operaciones de revocación y publicación según se establece en el punto 4.9.2. Los suscriptores podrán continuar utilizando certificados emitidos por esa ACPA hasta la fecha de expiración de los mismos o hasta que fueran revocados. El PSCA tiene la obligación de mantener los

servicios de revocación de certificados, publicación de CRL y/o validación OCSP durante ese lapso. Una vez expirados o revocados todos los certificados, y luego de notificada la UCE, cesa automáticamente la responsabilidad del PSCA para esa ACPA.

En caso de que el PSCA no pueda mantener la actividad de la ACPA durante el período de suspensión, quedan a criterio de la UCE las acciones a tomar.

4.12. Custodia (escrow) y recuperación de claves

4.12.1. Políticas y prácticas de custodia y recuperación de claves

Los PSCA, como Suscriptores de los certificados emitidos bajo la presente Política de Certificación, están autorizados a contratar servicios de *escrow* como respaldo para su clave privada. Los requerimientos para brindar servicios de escrowing de clave privada se encuentran publicados en el documento “Requerimientos para depositarios de clave privada de ACPA mediante escrow”, publicado en <https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados>.

Los PSCA se encuentran autorizados a almacenar copias de seguridad de su clave privada tomando las medidas de protección técnicas y físicas correspondientes (ver 6.2 – Protección de llave privada y controles de Módulos Criptográficos).

La recuperación de la clave privada, para continuar utilizando el mismo certificado, puede realizarse únicamente en los casos en los que la clave en posesión del PSCA haya sido destruida, por ejemplo, por fallas de hardware. El PSCA deberá notificar a la UCE de la situación y la ACRN deberá comprobar fehacientemente que no es posible reconstruir la clave privada y que no hay riesgo de que la misma se encuentre comprometida. Debe encontrarse presente personal designado por la ACRN en el procedimiento de recuperación de la clave.

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

No estipulado.

5. Gestión de las instalaciones y controles operacionales

El objetivo de los controles administrativos, operativos y físicos es implementar medidas de protección para la clave privada utilizada por la ACRN, la información de los PSCA y el ciclo de vida de los certificados emitidos por la ACRN y por las ACPA.

Los controles Administrativos, operativos y físicos deben estar documentados para su uso interno, y en la CPS de la Autoridad de Certificación (ACRN o ACPA) debe especificarse un resumen. La CPS estará sujeta a la aprobación de la UCE durante la acreditación inicial, mientras que la documentación interna estará sujeta a auditorías periódicas.

5.1. Controles físicos

La ACRN y las ACPA deberán implementar sólidas medidas de seguridad física para la protección de su equipamiento e instalaciones, tanto de accesos no autorizados como de siniestros como incendios e inundaciones.

Mínimamente se deben implementar los siguientes controles:

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

5.1.1. Localización del sitio y construcción

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

La instalación de los sistemas de CA de la ACRN se debe realizar durante la Ceremonia de Generación de Llaves de la ACRN. Durante dicho evento se instalan completamente los sistemas sobre el hardware de producción, y los requerimientos de atestiguamiento se detallan en el punto 6.2.1.

El equipamiento dedicado a la gestión de certificados del Prestador Acreditado (la CA misma) debe ser instalado en presencia de auditores autorizados, de forma de certificar su correcta instalación. Los PSCA podrán instalar su equipamiento en una fecha dada en presencia de auditores autorizados, y extraer del equipamiento una imagen de la instalación, la cual deberá ser enviada a la UCE y permanecer en poder de la misma hasta el momento de su ceremonia de generación de llaves. La misma también deberá ser auditada, y comprenderá el proceso de instalación de la imagen en los sistemas además de la posterior generación de los pares de llaves, tal como se expresa en el punto 6.2.2.

5.1.2. Acceso físico

La ACRN y las ACPAs deberán 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 ACRN y las ACPAs deberán asegurar que las provisiones de energía y aire acondicionados son suficientes para el correcto funcionamiento del ACPA.

5.1.4. Exposición del agua

La ACRN y las ACPAs deberán asegurar que sus sistemas están protegidos a la exposición del agua.

5.1.5. Prevención y protección contra incendios

La ACRN y las ACPAs deberán asegurar que sus sistemas están protegidos con un sistema de extinción de incendios.

5.1.6. Almacenamiento de medios

La ACRN y las ACPAs deberán 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 ACRN y las ACPAs deberán 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 (off-site)

La ACRN y las ACPAs deberán 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

Los procesos que permiten el funcionamiento de la ACRN y las ACPAs deberán estar documentados y deberán basarse en la contraposición de intereses para sus operaciones más críticas, interviniendo varias personas durante la solicitud, aprobación, ejecución y control de las tareas desarrolladas. Para aquellas tareas críticas como la gestión de la clave privada de la autoridad certificante, deben implementarse medidas de división del conocimiento y contraposición de intereses.

5.2.1. Roles de confianza

Cada PSCA y la ACRN deberán definir al menos los siguientes roles para la operación de sus ACPA y ACRN respectivamente:

- Custodio de clave;
- Oficial de Seguridad; y,
- Administrador de Sistemas.

Quienes desempeñen el rol de Custodio de clave tienen asignada la responsabilidad de proteger la clave privada de la ACPA o ACRN, 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 o la ACRN. Se entiende por procedimiento de activación de la clave privada, el procedimiento necesario para que la ACPA o la ACRN 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 o ACRN. 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 o ACRN.

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 o ACRN. En cualquier caso, el PSCA o ACRN será responsable porque siempre exista un conjunto de custodios de clave disponibles para activar la CA.

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 o ACRN, por esta razón este rol debe ser ejercido por personas de confianza del PSCA o del ACRN, seleccionadas de acuerdo con los procedimientos descritos en la sección 5.3. Los Custodios de clave deben firmar con el PSCA o ACRN 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 o ACRN 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 o ACRN.

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

5.3. Controles de personal

Los requerimientos de seguridad ligada al personal que empleen tanto la ACRN como las ACPA, deberán estar documentados, y además deberán estar especificados en sus respectivas Declaraciones de Prácticas de Certificación.

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:

- Ingreso de personal (políticas de selección, evaluación e inducción);
- 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.);
- Capacitación del personal (capacitación inicial y capacitaciones periódicas por rol, material utilizado para capacitación, planes de entrenamiento);
- Retiro temporal o definitivo del personal (bloqueo o eliminación de sus cuentas de usuario);
- Políticas para el trabajo de personal contratado (externo a la ACPA o ACRN);
- Política de sanciones para incumplimiento de las normas de seguridad de la ACPA o ACRN (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 o ACRN que ocupe roles de confianza debe estar libre de conflicto de intereses que puedan perjudicar la imparcialidad de las operaciones del ACPA o ACRN. La ACPA o ACRN 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 o ACRN 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.

Lo mismos requerimientos aplican para la ACRN-

5.3.4. Requerimientos y frecuencia de re-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.

Lo mismos requerimientos aplican para la ACRN-

5.3.5. Secuencia y frecuencia de rotación laboral

Las ACPAs y la ACRN 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, el ACPA o la ACRN.

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.

Lo mismos requerimientos aplican para la ACRN.

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

Tanto la ACRN como las ACPA deben tener definida una política de registros de auditoría (*logs*) que defina qué *operaciones* se registran y *cómo se* garantiza la integridad de esos registros. Mínimamente se deben registrar todas las actividades relativas a la gestión de claves (generación, destrucción, activación, desactivación, etc.), a la gestión de certificados (emisión, revocación, renovación, etc.) y a la emisión de CRLs y/o respuestas a consultas OCSP.

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:

- registro y procesamiento de solicitudes;
- emisión, renovación y revocación de certificados en la ACPA;
- generación de la clave privada -en caso de que aplique-;
- 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 (log)

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 (log) de auditoría

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 (log) 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 (log) 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 auditoría puede ser un componente interno. Los procesos de auditoría deben ser invocados al inicializarse el sistema y podrán terminar únicamente al apagar el sistema. El sistema de recolección de registros de auditoría debe asegurar la integridad y la disponibilidad de los datos recolectados. Si es necesario, el sistema de recolección de registros de auditoría 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 o ACRN deberá determinar si es necesario suspender las actividades del ACPA o ACRN 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

Para cada tipo de registro se debe especificar además qué política de retención se va a aplicar. Los registros relativos a la generación de claves y emisión/renovación de certificados deben mantenerse mínimamente hasta que el certificado expira o es revocado. Los registros relativos a las demás operativas deben mantenerse por al menos un (1) año. Los certificados emitidos por una autoridad certificadora deben ser mantenidos en su directorio público por tiempo indefinido, incluso luego de su expiración y/o revocación.

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, número de teléfono usado, personas con las que se habló 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 Prácticas de Certificación y versiones previas; y
- Acuerdos contractuales entre los Suscriptores y La ACRN y las ACPAs

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

El contenido del archivo deberá ser creado de tal manera que no pueda ser destruido ni borrado (a excepción de la transferencia a un medio de larga vida) por cualquier periodo de tiempo que se requiera retenerlo.

El archivo debe ser almacenado 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.

5.5.4. Procedimientos de respaldo del archivo

Deben implementarse procedimientos de respaldo del archivo y deben protegerse estos respaldos con los mismos requerimientos de seguridad que el archivo original.

5.5.5. Requerimientos para el sellado de tiempo (timestamp) 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

El cambio de claves se realiza con los procedimientos de Revocación y Emisión de Certificado en el mencionado orden o con el procedimiento de Renovación si es que la fecha de expiración es próxima.

Al renovar un ACPA su certificado, deberá divulgar la nueva clave publica como es estipulado en los puntos 6.1.3 y 6.1.4.

5.7. Compromiso y recuperación de desastres (continuidad de operaciones)

Tanto la ACRN como las ACPA deberán tener definidos planes de continuidad del negocio y recuperación ante desastres, que le permitan continuar con su operativa en la eventualidad de fallas de equipamiento y/o siniestros. El nivel mínimo de funcionamiento exigido para una autoridad certificadora en la PKI Uruguay es el de la atención de pedidos de revocación de certificados y provisión de los servicios de consulta de validez de los mismos.

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 de que ocurra un desastre o compromiso de un sistema o clave. Es especialmente crítica la continuidad de los servicios de revocación de certificados y publicación de CRL (ver sección 4.9).

Deben abordarse mínimamente los siguientes requerimientos:

7. Políticas para identificación de incidentes que puedan ocasionar un desastre en la operativa de la ACPA;
8. Procedimientos de recuperación para infraestructura y software en el caso de corrupción de datos;
9. Procedimientos para actuar en el caso de que la clave privada de la ACPA haya sido comprometida o se sospeche de su compromiso;

10. 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 cómputo, 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 con el plan de recuperación de desastres de la ACPA.

5.7.3. Procedimientos ante el compromiso de clave privada de entidad

En caso de 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], 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

Los controles técnicos descritos en esta sección tienen el objetivo de proteger el par de llaves de la ACRN y de las ACPA durante su ciclo de vida. Se especifican además medidas generales para la protección de los sistemas de información que dan soporte a las actividades de la ACRN y las ACPA.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

...4. Autoridad Certificadora Raíz Nacional

El par de llaves de la ACRN deberá ser generado durante la Ceremonia de Generación de Llaves. Dicha ceremonia se realiza en las instalaciones designadas por la AGESIC para la operación de la ACRN, bajo aprobación explícita de la UCE, respetando los requerimientos de la CPS de la ACRN y de acuerdo a lo estipulado en el Guion de la Ceremonia de Claves.

...5. Autoridad Certificadora del Prestador Acreditado

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

El PSCA debe contar con la infraestructura donde serán generadas las llaves previamente configuradas y las medidas de protección requeridas por la presente Política ya implementadas.

La generación del par de llaves debe realizarse en un módulo criptográfico seguro.

La llave generada deberá ser RSA de 4096 bits.

El PSCA debe elaborar previamente una guía donde se describa el procedimiento de generación de llaves y exportación del CSR. Deben especificarse en dicha guía las responsabilidades, pasos a seguir y registros formales de su ejecución.

Al finalizar el procedimiento, el funcionario designado por la ACRN debe retirar de las instalaciones del PSCA el CSR para ser posteriormente utilizado en la emisión del certificado.

6.1.2. Entrega de la clave privada al suscriptor

Las ACPAs generaran sus propias claves privadas.

6.1.3. Entrega de la clave pública al emisor del certificado

No aplica.

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

La ACRN debe publicar su clave pública en su repositorio de información. Se deben tomar medidas de protección adecuadas a nivel de sistemas para asegurar su integridad y prevención de ataques de sustitución.

6.1.5. Tamaños de clave

Como es estipulado en el punto 6.1.2 las claves para las ACPAs deberán ser RSA de 4096 bits con algoritmo de hash SHA-256 o superior, o bien Curvas Elípticas Nistp521 (521 bits), BrainpoolP512r1 (512 bits) o Ed448 (448 bits) con sus respectivos algoritmos de hash según se especifica en el punto 7.1.10.

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

La generación del par de llaves debe realizarse en un módulo criptográfico seguro como es estipulado en el punto 6.1.2 y 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)

- KeyCertSign
- CRLSign

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

6.2.1. Normas y controles para el módulo criptográfico

La protección de la llave privada de la ACRN y de las ACPA debe realizarse con módulos criptográficos (HSM) que cumplan con la normativa FIPS 140-2 nivel 3.

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

La ACRN y las ACPAs 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 (escrow) de la clave privada

El *escrow* de la llave maestra de las ACPA debe realizarse mediante un medio impreso con la llave codificada en base64. Ninguna persona ajena a la entidad que realiza el *escrow* puede tener acceso completo a ver o retener la llave maestra. Los procedimientos para *escrow* de llaves privadas son los detallados en la presente política (ver 4.12 - Recuperación y Escrow de la Llave).

Para que el respaldo o *escrow* de una llave privada sea efectivo, debe respaldarse la llave maestra del módulo criptográfico y la llave privada cifrada por dicha llave, o solo la llave privada en forma cifrada si el modelo particular de HSM no maneja llaves maestras.

No es permitido procedimientos de *escrow* para la ACRN.

6.2.4. Respaldo de la llave privada

La ACRN y las ACPAs podrá realizar respaldos de su llave privada bajo los mismos controles y procedimiento que los del *escrow* de la misma.

6.2.5. Archivo de la llave privada

La ACRN y las ACPAs no deben archivar la llave privada.

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

La llave maestra de la ACRN y de las ACPA no puede ser retirada de los módulos criptográficos en claro (sin cifrado). El cifrado a utilizar debe ser AES 256 o 3DES con llave de largo triple. El retiro de la llave maestra de los módulos de criptografía puede realizarse únicamente para procedimientos de respaldo de la llave, procedimientos de *escrow* (para el caso de las ACPA) y para el cambio de módulo criptográfico. Estos procedimientos deben ser aprobados y controlados según sea requerido en cada caso, por la UCE para el caso de la ACRN, y por la ACRN para el caso de las ACPA.

Las llaves maestras de un módulo criptográfico HSM que sean retiradas deben cifrarse con criptografía sólida, especificada en la CPS de la ACRN o de la ACPA según corresponda. La llave utilizada para la protección de la llave maestra retirada debe encontrarse dividida entre al menos 3 custodios, siendo cada custodio designado por la ACRN o la ACPA –según corresponda– y considerando la contraposición de intereses.

6.2.7. Almacenamiento de la llave privada en el módulo criptográfico

Las llaves privadas de la ACRN y de la ACPA pueden encontrarse únicamente cifradas bajo llaves generadas y residentes en los módulos criptográficos (llaves maestras). El

equipamiento de producción y el de contingencia (que es recomendable tener) deben contar con los controles de seguridad físicos y lógicos requeridos por esta Política de Certificación.

6.2.8. Método de activación de la clave privada

La ACRN y las ACPAs será responsable de activar la clave privada de acuerdo a las instrucciones y documentación provista por el proveedor del HSM.

6.2.9. Método de desactivación de la clave privada

La ACRN y las ACPAs deberán 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 línea 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

Una vez que el certificado de la ACRN o de la ACPA haya expirado, debe procederse a la destrucción de la clave privada y de la clave maestra del módulo criptográfico. La destrucción debe realizarse con un mecanismo que impida su recuperación. En caso de que se haya realizado *escrow* en un medio impreso, el método de destrucción es su incineración. En caso de una *smart-card*, debe destruirse físicamente de forma que no pueda ser reconstruida. El módulo de criptografía utilizado debe proveer funciones para la eliminación segura de la llave maestra.

La destrucción de la clave privada de la ACRN debe realizarse según los procedimientos estipulados en su CPS.

La destrucción de la clave privada de la ACPA es responsabilidad del PSCA acreditado. El PSCA debe contar con procedimientos para tales fines especificados en su Declaración de Prácticas de Certificación y, por lo tanto, aprobados por la UCE en el proceso de acreditación.

6.2.11. Clasificación del módulo 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 ACRN y los PSCA deberán mantener un archivo de todos los certificados que contengan claves públicas utilizadas para la emisión de certificados, es decir, todos los

certificados alguna vez utilizados por sus Autoridades de Certificación. De esta forma, es posible validar las cadenas de confianza en las que participan la ACRN o las ACPA para cualquier instante de tiempo.

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

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

El período de validez máximo de los certificados emitidos por la ACRN bajo la presente Política de Certificación (certificados de las ACPA) es el máximo posible al momento de la emisión, según la fecha de expiración del certificado de la ACRN (ver 4.3 - Emisión de Certificado).

El período de validez máximo del par de llaves de la ACRN o de la ACPA es el de su certificado. Transcurrido dicho período o en caso de revocación del certificado, la llave privada correspondiente a la llave pública contenida en el certificado debe ser eliminada (ver 6.2 – Protección de la llave privada y controles de Módulos Criptográficos).

6.4. Datos de activación

Se entiende por “activación” al proceso previo a la utilización de la llave privada que permite, mediante un mecanismo de autenticación, hacerla disponible para ser usada. Esto implica que la llave privada sea usada múltiples veces tras un único proceso de autenticación. La activación puede realizarse por ejemplo al iniciar el sistema. En el caso de las ACPA, se activa la llave privada al comenzar las actividades de emisión de certificados o CRLs firmadas.

Cuando la llave privada no sea utilizada o se cumpla alguna de las condiciones establecidas, debe ser desactivada. Se entiende por “desactivación” cualquier proceso que haga *imprescindible* volver a activar la llave privada para utilizarla. Por ejemplo, puede definirse que tras determinado período de inactividad del sistema o al apagarlo, se desactive la llave privada. En el caso de las ACPA, esto puede darse en el reinicio del sistema de emisión de certificados o en la suspensión del servicio por operaciones de mantenimiento. Los PSCA deben definir las condiciones para la desactivación de la llave privada en su Declaración de Prácticas de Certificación. Estas condiciones deben ser lo más restrictivas posibles de forma tal de evitar que la llave privada se encuentre activada mientras no esté siendo utilizada.

En la ACRN la llave privada debe activarse al iniciar el sistema para emitir una CRL o un certificado. La desactivación debe realizarse tras la emisión de la CRL o del certificado.

Los datos para la activación de una llave privada pueden ser un PIN, *token* o *passphrase*.

6.4.1. Generación e instalación de los datos de activación

La generación y uso de los datos de activación del ACPA y la ACRN usados para activar las claves privadas del ACPA y la ACRN, 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

Para la activación de las llaves privadas de la ACRN y de la ACPA se requiere la participación de varios individuos (custodios) en un esquema “N de M”. Esta división del conocimiento impide que un individuo por sí solo tenga el conocimiento suficiente para activar la llave privada. Para la ACRN N no deberá ser menor a tres, mientras que para las ACPA no deberá ser menor a dos.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

6.5. Controles de seguridad computacional

6.5.1. Requerimientos técnicos específicos de seguridad computacional

La ACRN y la ACPA deben implementar políticas, estándares y procedimientos que permitan una operación segura.

Se deben instrumentar como mínimo los siguientes aspectos:

- a) Definición de roles y responsabilidades;
- b) Clasificación de la información;
- c) Seguridad vinculada a los recursos humanos;
- d) Seguridad lógica de los sistemas y redes;
- e) Control del acceso lógico;
- f) Seguridad física del ambiente y de los sistemas;
- g) Gestión de respaldos;
- h) Continuidad de la operativa y disponibilidad;
- i) Registros de auditoría;

j) Respuesta a incidentes.

Estos controles serán objeto de regulación por parte de la UCE para la obtención y mantenimiento de la acreditación como PSCA.

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

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

Estos controles serán objeto de regulación por parte de la UCE para la obtención y mantenimiento de la acreditación como PSCA.

6.7. Controles de seguridad de la red

Deben implementarse medidas adecuadas de protección para la operación de la ACRN y las ACPA si se encuentran conectadas en red. Por ejemplo, división de la red de la organización en capas, ubicando la ACPA en un segmento crítico al que no sea posible el acceso desde Internet. Si la Autoridad de Registro de la ACPA cuenta con un portal *online* y además está conectada a la ACPA para la emisión de certificados *online*, esta conexión debe estar sujeta a estrictos controles de seguridad a nivel de red, como por ejemplo mediante firewalls, controles de acceso y auditoría (logs).

Estos controles serán objeto de regulación por parte de la UCE para la obtención y mantenimiento de la acreditación como PSCA.

6.8. Sellado de tiempo

La ACRN y las ACPA deben utilizar la fecha y hora GMT al firmar los certificados que emiten, con un margen de error máximo del orden del minuto.

7. Perfiles de Certificado y CRL

El formato del certificado cumple con lo especificado en el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), mientras que la lista de revocación de certificados cumple con el mismo estándar, pero en su versión 2. Ambos están definidos en su versión más reciente en el RFC 5280.

Adicionalmente, para el caso de uso de Curvas Elípticas, las mismas son definidas a través de: RFC 6979 para curvas NIST; RFC 5639 para curvas Brainpool y RFC 8032 para curvas Edwards.

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

7.1. Perfil de certificado

7.1.1. Número(s) de versión

Los certificados emitidos bajo esta política son certificados X.509 versión 3 [5].

7.1.2. Extensiones del certificado

Las extensiones de los certificados se estipulan en los perfiles

7.1.3. Identificadores de objeto de algoritmos

La ACRN deberá firmar los certificados emitidos 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 }
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}
ECCEncryption	{iso(1) identified-organization(3) thawte(101) id-Ed448(113)}

ECCEncryption	{iso(1) identified-organization(3) thawte(101) id-Ed25519(112)}
---------------	---

Si la ACRN 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 }

Las ACPAs podrán generar pares de claves usando los siguientes algoritmos:

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 }
ECCEncryption	{iso(1) identified-organization(3) thawte(101) id-Ed448(113)}
ECCEncryption	{iso(1) identified-organization(3) thawte(101) id-Ed25519(112)}

7.1.4. Formas de nombre

Los certificados emitidos bajo la presente política 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 [6].

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.

7.1.5. Restricciones de nombres

No es aplicable. Los certificados emitidos bajo la presente política no utilizan la extensión Name Constraints.

7.1.6. Identificadores de objeto de política de certificación

En la extensión Certificate Policies se utilizarán el OID { joint-iso-ccitt(2) country(16) uy(858) 10000157 66565 0 } para mostrar adhesión a la presente política. También en

dicha extensión se utilizarán el OID asignados a las CPS bajo la cual se emitió el certificado, actualmente { joint-iso-ccitt(2) country(16) uy(858) 10000157 66565 1 } .

7.1.7. Uso de la extensión “Policy Constraints”

No se utiliza la extensión “Policy Constraints” en los certificados del ACPA o la ACRN.

7.1.8. Sintaxis y semántica de calificadores de política

Se utilizarán los calificadores definidos en el RFC5280 [6]. Particularmente se utilizará el calificador “CPS Pointer qualifier” donde se colocará la URI en la que se accede al documento.

7.1.9. Semántica de procesamiento para la extensión crítica “Certificate Policies”.

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

7.1.10. Perfiles

...6. Perfil de certificado de la ACRN

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

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACRN
Algoritmo de Firma (Signature Algorithm)	sha256RSA SHA384RSA sha512RSA ECC-Brainpool (conforme RFC 5639) Curve25519 (Conforme RFC 7748) Ed25519 (PureEdDSA o HashEdDSA conforme RFC 8032) sha256WithECDSAEncryption sha512WithECDSAEncryption Ed448-Goldilocks (PureEdDSA y HashEdDSA, conforme RFC 8032.

Nombre Distintivo del Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Validez (Valid From / Valid To)	20 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 4096 bits Nistp521 (521 bits) BrainpoolP512r1 (512 bits) Ed448 (448 bits)

Extensiones:

Atributos	Criticidad	Contenido
Identificador de la clave del suscriptor (Subject Key Identifier)	No critica.	Hash de 20 bytes del atributo Subject Public Key
Uso de Claves (Key Usage)	CRITICA	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	No critica	OID: 2.16.858.10000157.66565.0 URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/cp_acrn_v2.2.pdf OID: 2.16.858.10000157.66565.1 URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/DeclaracionPracticasCertificacionAutoridadCertificadoraRaizUruguay_v2_1.pdf

Restricciones Básicas (Basic Constraints)	CRITICA	CA = TRUE Largo indefinido
Puntos de distribución de las CRL (CRL Distribution Points)	No critica	URI = www.agesic.gub.uy/acrn/acrn.crl URI = www.uce.gub.uy/acrn/acrn.crl

...7. Perfil de certificado de las ACPA

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

Atributos	Contenido
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACRN
Algoritmo de Firma (Signature Algorithm)	sha256RSA sha512RSA SHA384RSA ECC-Brainpool (conforme RFC 5639) Curve25519 (conforme RFC 7748) Ed25519 (PureEdDSA o HashEdDSA conforme RFC 8032) sha256WithECDSAEncryption sha512WithECDSAEncryption Ed448-Goldilocks (PureEdDSA y HashEdDSA, conforme RFC 8032)
Nombre Distintivo del Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Validez (Valid From / Valid To)	Período de validez asignado al momento de la emisión (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	Nombre Distinguido de la ACPA según lo establecido en el punto 3.1.1
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 4096 bits Nistp521 (521 bits) BrainpoolP512r1 (512 bits)

Ed448 (448 bits)

Extensiones:

Atributos	Criticidad	Contenido
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	No Critica	Identificador de la clave pública de la ACRN
Identificador de la clave del suscriptor (Subject Key Identifier)	No critica	Hash de 20 bytes del atributo Subject Public Key
Uso de Claves (Key Usage)	CRITICA	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	No critica	OID: 2.16.858.10000157.66565.0 URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/cp_acrn_v2.2.pdf OID: 2.16.858.10000157.66565.1 URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/DeclaracionPracticasCertificacionAutoridadCertificadoraRaizUruguay_v2_1.pdf
Restricciones Básicas (Basic Constraints)	CRITICA	CA = TRUE Largo 0
Puntos de distribución de las CRL (CRL Distribution Points)	No critica	URI = www.agesic.gub.uy/acrn/acrn.crl URI = www.uce.gub.uy/acrn/acrn.crl
Información de Acceso de la Autoridad Certificadora (Authority Information Access)	No critica	URI = www.agesic.gub.uy/acrn/acrn.cer

7.2. Perfil de la CRL de la ACRN

7.2.1. Número(s) de versión

Para la emisión de las CRL de la ACRN se utilizará el formato X.509 versión 2.

7.2.2. CRL y Extensiones de entradas CRL

Se utilizarán los siguientes campos del formato X.509 versión 2[5]:

Atributos	Contenido
Versión (Version)	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA sha512RSA sha384RSA Nistp521 (521 bits) BrainpoolP512r1 (512 bits) Ed448 (448 bits)
Nombre Distintivo del Emisor (Issuer DN)	CN = Autoridad Certificadora Raíz Nacional de Uruguay O = AGESIC C = UY
Día y Hora de Emisión (Effective Date)	Día y hora de la emisión de esta CRL
Próxima Actualización (Next Update)	Día y hora de la próxima actualización planificada de la CRL (3 meses)
Certificados Revocados (Revoked Certificates)	Lista de los certificados revocados. Incluye número de serie (Serial Number) y fecha de revocación (Revocation Date).
Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Identificador de la clave pública de la ACRN
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

7.3. Perfil OCSP

7.3.1. Número(s) de versión

No aplica.

7.3.2. Extensiones OCSP

No aplica.

8. Auditoria de cumplimiento y otras evaluaciones

8.1. Frecuencia o circunstancias de evaluación

La UCE se encuentra sujeta a auditorias periódicas. La información relevante de los informes de las auditorías es publicada en el sitio web de publicación de la UCE.

La ACRN se encuentra sometida a auditorías de la UCE y de auditores independientes y autorizados. La frecuencia para dichas auditorias es estipulada por la UCE. La información relevante de los informes de las auditorías es publicada en el sitio web de publicación de la UCE y deberá ser publicada en el sitio de publicación de la ACRN.

Los Prestadores de Servicios de Certificación deberán someterse a una auditoria por un auditor autorizado, previo a la acreditación, como lo estipula el decreto N° 436/011, de 8 de diciembre de 2011 expresamente en su artículo 13 literal E.

Luego de la acreditación los PSCA deberán someterse a auditorías periódicas cuyos lineamientos y frecuencia estipula 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.

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. Los mismos son:

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

8.3. Relación del evaluador con la entidad evaluada

El evaluador deberá ser un auditor independiente.

8.4. Tópicos cubiertos por la evaluación

La auditoría debe cumplir con los requerimientos del esquema de auditoria bajo el cual la evaluación se está realizando (por ejemplo Web Trust). Los esquemas de auditoria

pueden ser actualizados, por lo que un esquema de auditoria será aplicable a la ACRN o las ACPAs en el año próximo a la adopción del nuevo esquema.

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

No se percibirá contraprestación económica por la emisión de certificados por parte de la ACRN a los PSCA.

9.1.2. Tarifas de acceso a los certificados

La ACRN no debe percibir tarifas por acceso a certificados.

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

La ACRN no debe percibir tarifas por otros servicios.

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

A los efectos de la determinación del carácter de confidencial de la información recibida por la UCE se estará a los recaudos previstos de acuerdo con lo establecido en la Ley N° 18.381, de 17 de octubre de 2008.

La información personal queda regulada por las Leyes Nos. 18.331, de 11 de agosto de 2008.

9.3.2. Información fuera del alcance de la información confidencial

La siguiente información referida a los PSCA se hará pública por parte de la UCE:

- a) Los datos de contacto de los PSCA;
- b) La información sobre el resultado de la auditoría de los PSCA;
- c) Los requerimientos para la acreditación de los PSC;
- d) Las resoluciones mediante las que se acredita, suspende, renueva, revoca o deniega la acreditación a los PSC.

La información referida a la revocación de un certificado no se considera confidencial y deberá ser publicada por la ACRN a través de su CRL, publicada en el sitio <http://www.uce.gub.uy/acrn/acrn.crl> (la URL concreta deberá estar especificada en la CPS de la ACRN). Las razones que dan lugar a una revocación se consideran públicas, y estarán incluidas en el repositorio público de la UCE (<https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados>).

La información sobre el estado de suspensión de un PSCA no se considera confidencial y se publica en el repositorio público de la UCE: <https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados>. De la misma forma, las razones que dan lugar a la suspensión estarán incluidas en el repositorio público de la UCE, en la misma URL.

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

9.4.1. Plan de privacidad

No estipulado.

9.4.2. Información personal

La información personal queda regulada de acuerdo con lo dispuesto por las Leyes Nos. 18.331, de 11 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 N° 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 aquella especialmente determinada como secreta por Ley, reservada y confidencial.

9.4.4. Responsabilidad de proteger información privada

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

9.4.5. Aviso y consentimiento de usar información privada

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del PSCA o de cualquier otra información generada o recibida durante el ciclo de vida del certificado solo se hará efectiva previa autorización de dicho PSCA. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público.

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 jurisdiccional.

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 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 registrarán por lo dispuesto en la normativa nacional vigente.

Sin perjuicio de lo señalado, las CAs 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 N° 18.600 y el Decreto N° 436/011.

9.6.2. Declaraciones y garantías de la RA

Las garantías se registrarán 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 - que en el marco de la presente política serán las ACPAs - deberán cumplir con las obligaciones estipuladas en 9.17.2.3

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 del ACPA es válido y fue emitido por la ACRN.
- 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 la ACRN a la fecha de la validación.
- D) El certificado de la ACRN es válido de acuerdo con la presente Política.
- E) El certificado se está utilizando para uno de los usos permitidos en la Política de Certificación correspondiente.

Adicionalmente los terceros aceptantes deberán cumplir con las obligaciones estipuladas en 9.17.2.5.

9.6.5. Declaraciones y garantías de los demás participantes

No aplica.

9.7. Renuncia de garantías

No aplica.

9.8. Limitaciones de responsabilidad

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.

9.9. Indemnizaciones

No aplica.

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.

El sistema documental y de organización de la UCE tendrá que garantizar, a través de la existencia y de la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la Política de Certificación y de las especificaciones del servicio relacionadas con ella. Se prevén, de esta forma, el procedimiento de modificación de especificación del servicio y el procedimiento de publicación de especificaciones del servicio. Las modificaciones finales de la Política de Certificación tendrán que ser aprobadas por la UCE, después de comprobar el cumplimiento de los requisitos establecidos en las secciones correspondiente de esta política.

9.12.2. Procedimiento de enmiendas

No aplica.

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

Ante cambios de versiones mayores en la presente política de certificación, se le asignará un nuevo OID identificadorio.

9.13. Disposiciones de resolución de disputas

Los PSCA en su calidad de suscriptores de certificados emitidos por la ACRN y los Terceros aceptantes de dichos certificados podrán interponer un recurso administrativo ante la UCE por conflictos referidos a la prestación del servicio.

9.14. Ley aplicable

La interpretación, obligatoriedad, estructura y validez de esta Política de Certificación se encuentran regidas por la Ley No 18.600 y demás normas aplicables.

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. Obligaciones

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

...8. Obligaciones de la UCE

Constituyen obligaciones de la UCE en relación con la presente política:

- a) La elaboración o aprobación, actualización y cancelación de las políticas de certificación de la PKI Uruguay;
- b) La acreditación de los PSC para operar dentro de la PKI Uruguay;
- c) La publicación de la lista de PSC Acreditados a operar en PKI Uruguay;
- d) El control y auditoría de los PSCA para garantizar que sus prácticas cumplen con las políticas de certificación para las cuales fueron acreditados, la presente Política de Certificación, su Declaración de Prácticas de Certificación y la normativa legal vigente;
- e) La publicación en el Sitio Oficial, y referencia en el Diario Oficial, de:
 - 1. La Resolución que ordena el otorgamiento, denegación, renovación, suspensión y/o revocación de acreditación para un PSC, y
 - 2. El certificado electrónico emitido por la ACRN a la ACPA bajo la presente Política;
 - 3. La modificación de la presente Política de Certificación.
- f) Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad o confidencialidad según corresponda);
- g) Mantener a disposición permanente del público las políticas de certificación de la PKI Uruguay;
- h) Disponer de un servicio de atención que permita responder las consultas de los suscriptores de certificados emitidos por los PSCA y los Terceros aceptantes de dichos certificados;

- i) Atender los requerimientos de revocación de certificados solicitados por los PSCA o por una autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;
- j) Atender los requerimientos de suspensión de un PSCA por parte de una autoridad competente, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;
- k) La publicación de la Lista de PSCA Suspendidos en su repositorio de información;
- l) Notificar a los PSCA, como suscriptores de los certificados emitidos por la ACRN bajo la presente política, acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACRN y la emisión de un nuevo par de claves criptográficas, como también del procedimiento a seguir en ese caso;
- m) Desarrollar, mantener y actualizar procedimientos que permitan la realización de sus actividades en cumplimiento con la presente Política de Certificación y la normativa legal vigente.

...9. Obligaciones de la ACRN

Constituyen obligaciones de la ACRN:

- a) Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, en conformidad con lo pautado en la presente Política;
- b) Notificar a la UCE ante cualquier operación;
- c) Generar su clave privada con aprobación de la UCE y según lo pautado en el Guion de Ceremonia de Claves;
- d) Proteger su clave privada;
- e) Emitir y renovar su propio certificado con aprobación de la UCE y según lo pautado en el Guion de Ceremonia de Claves;
- f) Revocar su propio certificado ante sospecha real de compromiso de la clave privada asociada;
- g) Atender los requerimientos de revocación de certificados solicitados por los PSCA o por la UCE, de acuerdo con la legislación vigente y los procedimientos definidos en la presente Política de Certificación;

- h) Utilizar el certificado de la ACRN de acuerdo con los requerimientos de la presente política de certificación;
- i) La emisión, revocación y renovación de los certificados de las ACPA;
- j) La emisión y publicación de su Lista de Certificados Revocados (CRL);
- k) El envío a la UCE de las CRL inmediatamente después de emitidas;
- l) Notificar a los PSCA, como suscriptores de los certificados emitidos por la ACRN bajo la presente política, acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACRN y la emisión de un nuevo par de claves criptográficas, como también del procedimiento a seguir en ese caso;
- m) Garantizar el acceso permanente y gratuito de los suscriptores y Terceros aceptantes al sitio de publicación que contiene su propio certificado, los certificados emitidos a los PSCA y la lista de certificados revocados;
- n) Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad o confidencialidad según corresponda).

...10. Obligaciones de los PSCA

Los PSCA son personas físicas o jurídicas, públicas o privadas, nacionales o extranjeras, que expiden certificados electrónicos reconocidos u otros servicios en el marco de PKI Uruguay, bajo cuya responsabilidad recaerán las obligaciones citadas en este punto.

Toda la información necesaria para la identificación y autenticación del PSC a acreditar contenida en una solicitud de acreditación debe ser provista de forma completa y precisa al iniciar el proceso de acreditación. Dicha información se encuentra disponible en el Procedimiento para la acreditación como Prestador de Servicios de Certificación de PKI Uruguay, en <https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/prestadores-acreditados>.

Al aceptar un certificado emitido por la ACRN para su ACPA, el PSCA es responsable de toda la información por él provista y contenida en ese certificado.

La ACPA asociada al certificado emitido por la ACRN debe operar de acuerdo con su propia Declaración de Prácticas de Certificación (CPS), previamente aprobada por la UCE, y a las Políticas de Certificación de PKI Uruguay para las cuales se acreditó ante la UCE.

Los PSCA asumen las siguientes obligaciones:

- a) Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, en conformidad con lo pautado en la presente Política y demás normativa vigente aplicable;
- b) Proveer toda la información que le sea requerida de modo completo y preciso a fines de obtener el certificado emitido por la ACRN para su ACPA bajo la presente política de certificación;
- c) Generar la clave privada de su ACPA en las condiciones establecidas en el punto 6.2.2;
- d) Proteger la clave privada de su ACPA;
- e) Solicitar la inmediata revocación del certificado emitido por la ACRN en el caso de compromiso o sospecha de compromiso de la clave privada de su ACPA;
- f) Utilizar el certificado de su ACPA de acuerdo con los requerimientos de la presente política de certificación;
- g) Mantener un sitio web donde publique de forma actualizada la información de acreditación ante la UCE, el certificado emitido por la ACRN a su ACPA y la información requerida por las políticas de certificación para las que se haya acreditado ante la UCE;
- h) Publicar en dicho sitio web la Lista de Revocación de Certificados (CRL, por sus siglas en inglés) para los certificados que emita, de acuerdo a la reglamentación vigente;
- i) Enviar diariamente la Lista de Revocación de Certificados a la UCE, en concordancia con la normativa vigente;
- j) Cumplir con las obligaciones establecidas en la presente política de certificación, las políticas de certificación para las cuales se acredita y otros documentos aplicables emitidos por la UCE;
- k) Firmar el Acuerdo con Suscriptores de Certificados de la ACRN, al aceptar el certificado emitido por la ACRN.

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

Las obligaciones de Autoridad de Registro de la ACRN son asumidas por la AGESIC:

- a) Comprobar la validez de la acreditación para los PSCA que solicitan la emisión, revocación o renovación de un certificado;

- b) Procesar las solicitudes de emisión, renovación o revocación de certificados emitidos por la ACRN;
- c) Notificar a los PSCA ante la ocurrencia de un evento que así lo requiera según lo estipulado por la presente Política de Certificación;
- d) Mantener un repositorio público de información de acuerdo al requerimiento 2.1 – Obligaciones del servicio de repositorio de la PKI Uruguay de la presente Política de Certificación.

El proceso de Acreditación de un Prestador de Servicios de Certificación se encuentra descrito en el documento “Procedimiento para la acreditación como Prestador de Servicios de Certificación de PKI Uruguay”, publicado por la UCE en su sitio web (www.uce.gub.uy/informacion-tecnica/prestadores).

9.17.4. Obligaciones de los Terceros Aceptantes

Los Terceros aceptantes tienen las siguientes obligaciones:

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

- a) garantías y usos aceptables del certificado de la ACRN;
- b) garantías y usos aceptables de los certificados emitidos por la ACRN a las ACPA;
- c) obligaciones de los Terceros aceptantes
- d) Tomar conocimiento y aceptar los términos definidos en la política de certificación bajo la cual el PSCA le emitió el certificado al suscriptor final;
- e) Verificar la validez del certificado de la ACRN. El certificado de la ACRN es considerado válido cuando:
- f) Se encuentra dentro de su período de vigencia,
- g) Su firma electrónica avanzada puede ser verificada con el uso del mismo certificado de la ACRN, y
- h) No ha sido revocado según la CRL publicada por la ACRN.
- i) Verificar la validez de los certificados emitidos por la ACRN a las ACPA. El certificado es considerado válido cuando;

- j) Se encuentra dentro de su período de vigencia,
- k) Su firma electrónica puede ser verificada con la clave pública del certificado de la ACRN, y
- l) No ha sido revocado según la CRL publicada por la ACRN.
- m) Verificar que el certificado 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 emitido por un PSCA 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: Unidad de Certificación Electrónica, Política de Certificación de la Autoridad Certificadora Raíz Nacional, 2011
- 4: Poder Legislativo, República Oriental del Uruguay, Ley N° 18.600 de Documento Electrónico , 21 de setiembre de 2009
- 5: 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
- 6: Cooper, Santesson, Farrell, Boeyen, Housley, Polk, RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008