



# **Declaración de Prácticas de Certificación (CPS) de la ACEDICOM**

Redactada siguiendo las especificaciones del RFC 3647 y completada  
con puntualizaciones de la ETSI TS 101 456 V1.2.1

**Fecha:** 27/08/2008 **Versión:** 1.4

**Estado:** VIGENTE **Nº de páginas:** 62

**OID:** 1.3.6.1.4.1.30051.2.1.1.1 **Clasificación:** PUBLICO

**Archivo:** ACEDICOM - PracticasCertificacion.doc

**Preparado por:** Autoridad de Certificación EDICOM - ACEDICOM

<b>Historial de cambios</b>			
<b>Versión</b>	<b>Fecha</b>	<b>Descripción de la acción</b>	<b>Páginas / Secciones</b>
1.0	07/05/2008	Inicial	
1.1	15/05/2008	Cambios menores por recomendación de auditoría de S21SEC	
1.2	30/05/2008	Cambio menor. Aclaración funciones del rol Administrador de HSM	
1.3	27/06/08	Cambio menor. Ampliación de políticas de seguridad	
1.4	27/08/08	Cambios según comentarios del Ministerio de Industria y Comercio	1.6.1, 3.1.1, 3.2.3, 4.9.3, 4.9.9, 5.4.3, 6.3.1, 9.6.1.2, 9.11.1

## Tabla de Contenido

<b>1. INTRODUCCIÓN .....</b>	<b>10</b>
<b>1.1. PRESENTACIÓN.....</b>	<b>10</b>
<b>1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN.....</b>	<b>12</b>
<b>1.3. PARTICIPANTES DE LA PKI, COMUNIDAD DE USUARIOS CERTIFICADOS.....</b>	<b>12</b>
1.3.1. Autoridades de Certificación.....	12
1.3.2. Autoridades de Registro .....	13
1.3.3. Usuarios finales .....	14
<b>1.4. USO DE LOS CERTIFICADOS .....</b>	<b>15</b>
1.4.1 Usos típicos de los certificados .....	15
1.4.2. Usos prohibidos .....	16
1.4.3. Fiabilidad de la firma electrónica a lo largo del tiempo .....	16
<b>1.5. ADMINISTRACIÓN DE LAS POLÍTICAS .....</b>	<b>17</b>
1.5.1. Organización responsable del CPS.....	17
1.5.2. Persona de Contacto para el CPS .....	17
1.5.3. Competencia para determinar la adecuación de la CPS con las diferentes Políticas de certificación.....	17
1.5.4 Procedimiento de aprobación.....	17
<b>1.6. DEFINICIONES Y ACRÓNIMOS.....</b>	<b>17</b>
1.6.1. Definiciones .....	17
1.6.2. Acrónimos.....	20
<b>2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS</b>	<b>21</b>
<b>2.1. REPOSITORIOS .....</b>	<b>21</b>
<b>2.2. PUBLICACIÓN .....</b>	<b>21</b>
<b>2.3. FRECUENCIA DE ACTUALIZACIONES .....</b>	<b>21</b>
<b>2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....</b>	<b>21</b>
<b>3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS .....</b>	<b>23</b>
<b>3.1. REGISTRO DE NOMBRES .....</b>	<b>23</b>
3.1.1. Tipos de nombres .....	23
3.1.2. Significado de los nombres .....	23
3.1.3. Interpretación de formatos de nombres.....	24
3.1.4. Unicidad de los nombres .....	24
3.1.5. Resolución de conflictos relativos a nombres .....	24
3.1.6. Reconocimiento, autenticación y función de las marcas registradas.....	24

<b>3.2. VALIDACIÓN DE LA IDENTIDAD INICIAL .....</b>	<b>24</b>
3.2.1.Métodos de prueba de posesión de la clave privada.....	24
3.2.2.Autenticación de la identidad de una organización.....	24
3.2.3.Autenticación de la identidad de un individuo.....	26
<b>3.3. IDENTIFICACION Y AUTENTICACION DE LAS SOLICITUDES DE RENOVACION DE CLAVE. ....</b>	<b>26</b>
3.3.1.Identificación y autenticación de las solicitudes de renovación rutinarias.....	26
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave.....	26
después de una revocación – Clave no comprometida.....	26
<b>3.4. IDENTIFICACION Y AUTENTICACION DE LAS SOLICITUDES DE REVOCACION DE LA CLAVE .....</b>	<b>26</b>
 <b>4. EL CICLO DE VIDA DE LOS CERTIFICADOS.....</b>	 <b>28</b>
<b>4.1. SOLICITUD DE CERTIFICADOS.....</b>	<b>28</b>
<b>4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....</b>	<b>28</b>
<b>4.3. EMISIÓN DE CERTIFICADOS .....</b>	<b>28</b>
<b>4.4. ACEPTACIÓN DE CERTIFICADOS .....</b>	<b>28</b>
<b>4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....</b>	<b>29</b>
<b>4.6. RENOVACIÓN DE CERTIFICADOS.....</b>	<b>29</b>
<b>4.7. RENOVACIÓN DE CLAVES .....</b>	<b>29</b>
<b>4.8. MODIFICACIÓN DE CERTIFICADOS. ....</b>	<b>29</b>
<b>4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....</b>	<b>29</b>
4.9.1.Circunstancias para la revocación.....	29
4.9.2.Entidad que puede solicitar la revocación.....	30
4.9.3.Procedimiento de solicitud de revocación.....	30
4.9.4.Periodo de gracia de la solicitud de revocación.....	30
4.9.5.Circunstancias para la suspensión.....	30
4.9.6.Entidad que puede solicitar la suspensión.....	30
4.9.7.Procedimiento para la solicitud de suspensión.....	30
4.9.8.Límites del período de suspensión.....	30
4.9.9.Frecuencia de emisión de CRLs.....	31
4.9.10.Requisitos de comprobación de CRLs.....	31
4.9.11.Otras formas de información de los certificados revocados.....	31
4.9.12.Requisitos especiales de renovación de claves comprometidas.....	31
<b>4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....</b>	<b>31</b>
4.10.1. Características operativas.....	31
4.10.2. Disponibilidad del servicio.....	31
<b>4.11.FINALIZACIÓN DE LA SUSCRIPCIÓN.....</b>	<b>32</b>
<b>4.12.DEPÓSITO Y RECUPERACIÓN DE CLAVES.....</b>	<b>32</b>

<b>5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES</b>	<b>33</b>
<b>5.1. CONTROLES DE SEGURIDAD FÍSICA</b>	<b>33</b>
5.1.1. Ubicación y construcción	33
5.1.2. Acceso físico	33
5.1.3. Alimentación eléctrica y aire acondicionado	33
5.1.4. Exposición al agua	33
5.1.5. Protección y prevención de incendios	34
5.1.6. Sistema de almacenamiento	34
5.1.7. Eliminación de residuos	34
5.1.8. Backup remoto	34
<b>5.2. CONTROLES DE PROCEDIMIENTOS</b>	<b>34</b>
5.2.1. Papeles de confianza	34
5.2.2. Número de personas requeridas por tarea	35
5.2.3. Identificación y autenticación para cada papel	35
<b>5.3. CONTROLES DE SEGURIDAD DE PERSONAL</b>	<b>35</b>
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación	36
5.3.2. Procedimientos de comprobación de antecedentes	36
5.3.3. Requerimientos de formación	36
5.3.4. Requerimientos y frecuencia de actualización de la formación	36
5.3.5. Frecuencia y secuencia de rotación de tareas	36
5.3.6. Sanciones por acciones no autorizadas	36
5.3.7. Requerimientos de contratación de personal	37
5.3.8. Documentación proporcionada al personal	37
5.3.9. Controles periódicos de cumplimiento	37
5.3.10. Finalización de los contratos	37
<b>5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD</b>	<b>38</b>
5.4.1. Tipos de eventos registrados	38
5.4.2. Frecuencia de procesado de logs	38
5.4.3. Periodo de retención para los logs de auditoría	38
5.4.4. Protección de los logs de auditoría	38
5.4.5. Procedimientos de backup de los logs de auditoría	38
5.4.6. Sistema de recogida de información de auditoría (interno vs externo)	38
5.4.7. Notificación al sujeto causa del evento	39
5.4.8. Análisis de vulnerabilidades	39
<b>5.5. ARCHIVO DE INFORMACIONES Y REGISTROS</b>	<b>39</b>
5.5.1. Tipo de informaciones y eventos registrados	39
5.5.2. Periodo de retención para el archivo	39
5.5.3. Protección del archivo	39
5.5.4. Procedimientos de backup del archivo	39
5.5.5. Requerimientos para el sellado de tiempo de los registros	40
5.5.6. Sistema de recogida de información de auditoría (interno vs externo)	40
5.5.7. Procedimientos para obtener y verificar información archivada	40
<b>5.6. CAMBIO DE CLAVE DE LA AC</b>	<b>40</b>
<b>5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE</b>	<b>40</b>
5.7.1. Alteración de los recursos hardware, software y/o datos	40

5.7.2.La clave pública de una entidad se revoca .....	40
5.7.3.La clave de una entidad se compromete.....	41
5.7.4.Instalación de seguridad después de un desastre natural u otro tipo de .....	41
desastre .....	41
<b>5.8. CESE DE UNA CA.....</b>	<b>41</b>
<b>6. CONTROLES DE SEGURIDAD TÉCNICA.....</b>	<b>42</b>
<b>6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES .....</b>	<b>42</b>
6.1.1.Generación del par de claves .....	42
6.1.2.Entrega de la clave privada a la entidad .....	42
6.1.3.Entrega de la clave publica al emisor del certificado .....	42
6.1.4.Entrega de la clave pública de la CA a los usuarios .....	42
6.1.5.Tamaño de las claves.....	42
6.1.6.Parámetros de generación de la clave pública .....	42
6.1.7.Comprobación de la calidad de los parámetros .....	42
6.1.8.Hardware/software de generación de claves .....	43
6.1.9.Fines del uso de la clave .....	43
<b>6.2. PROTECCIÓN DE LA CLAVE PRIVADA .....</b>	<b>43</b>
6.2.1.Estándares para los módulos criptográficos .....	43
6.2.2.Control multipersona de la clave privada .....	43
6.2.3.Custodia de la clave privada .....	43
6.2.4.Copia de seguridad de la clave privada .....	44
6.2.5.Archivo de la clave privada .....	44
6.2.6.Introducción de la clave privada en el módulo criptográfico.....	44
6.2.7.Método de activación de la clave privada.....	44
6.2.8.Método de desactivación de la clave privada.....	44
6.2.9.Método de destrucción de la clave privada .....	44
6.2.10 Clasificación de los módulos criptográficos.....	44
<b>6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....</b>	<b>44</b>
6.3.1.Archivo de la clave pública .....	44
6.3.2.Periodo de uso para las claves públicas y privadas.....	45
<b>6.4. DATOS DE ACTIVACIÓN .....</b>	<b>45</b>
6.4.1.Generación y activación de los datos de activación.....	45
6.4.2.Protección de los datos de activación .....	45
6.4.3.Otros aspectos de los datos de activación.....	45
<b>6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.....</b>	<b>45</b>
6.5.1 Requisitos técnicos específicos de seguridad informática .....	45
6.5.2 Evaluación del nivel de seguridad informática .....	46
<b>6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....</b>	<b>46</b>
6.6.1 Controles de desarrollo de sistemas .....	46
6.6.2 Controles de gestión de seguridad.....	46
<b>6.7. CONTROLES DE SEGURIDAD DE LA RED.....</b>	<b>46</b>
<b>6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS.....</b>	<b>46</b>

<b>7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS</b>	<b>47</b>
<b>7.1. PERFIL DE CERTIFICADO</b>	<b>47</b>
7.1.1. Número de versión	47
7.1.2. Extensiones del certificado	47
7.1.3. Identificadores de objeto (OID) de los algoritmos	47
7.1.4. Formatos de nombres	47
7.1.5. Restricciones de los nombres	48
7.1.6. Identificador de objeto (OID) de la Política de Certificación	48
7.1.7. Uso de la extensión "Policy Constraints"	48
7.1.8. Sintaxis y semántica de los cualificadores de política	48
7.1.9. Tratamiento semántico para la extensión crítica "Certificate Policy"	48
<b>7.2. Perfil de CRL</b>	<b>48</b>
7.2.1. Número de versión	48
7.2.2. CRL y extensiones	48
<b>7.3 LISTAS DE CERTIFICADOS REVOCADOS</b>	<b>48</b>
7.3.1 Limite Temporal de los certificados en las CRLs	48
<b>7.4.- PERFIL DE OCSP</b>	<b>48</b>
7.4.1.- Perfil del certificado OCSP responder	48
7.4.2.- Número de versión	49
7.4.3.- Formatos de nombres	49
7.4.4.- Identificador de objeto (OID) de la Política de Certificación	49
7.4.5.- Extensiones y campos del certificado	49
7.4.6.- Formato peticiones OCSP	50
7.4.7.- Formato de las respuestas	50
<b>8. AUDITORÍA DE CONFORMIDAD</b>	<b>51</b>
<b>8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD</b>	<b>51</b>
<b>8.2. IDENTIFICACION/CUALIFICACIÓN DEL AUDITOR</b>	<b>51</b>
<b>8.3. RELACION ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA</b>	<b>51</b>
<b>8.4. TOPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD</b>	<b>51</b>
<b>8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA</b>	<b>51</b>
<b>8.6. COMUNICACIÓN DE RESULTADOS</b>	<b>52</b>
<b>9. REQUISITOS COMERCIALES Y LEGALES</b>	<b>53</b>
<b>9.1. TARIFAS</b>	<b>53</b>
9.1.1. Tarifas de emisión de certificado o renovación	53
9.1.2. Tarifas de acceso a los certificados	53
9.1.3. Tarifas de acceso a la información de estado o revocación	53
9.1.4. Tarifas de otros servicios como información de políticas	53
9.1.5. Política de reintegros	53

<b>9.2. CAPACIDAD FINANCIERA.....</b>	<b>53</b>
9.2.1.Indemnización a los terceros que confían en los certificados emitidos por la ACEDICOM.....	53
9.2.2.Relaciones fiduciarias.....	53
9.2.3.Procesos administrativos.....	53
<b>9.3. POLÍTICA DE CONFIDENCIALIDAD .....</b>	<b>54</b>
9.3.1.Información confidencial.....	54
9.3.2.Información no confidencial.....	54
9.3.3.Divulgación de información de revocación /suspensión de certificados .....	54
<b>9.4. PROTECCIÓN DE DATOS PERSONALES.....</b>	<b>54</b>
9.4.1.Plan de Protección de Datos Personales.....	54
9.4.2.Información considerada privada.....	55
9.4.3.Información no considerada privada.....	55
9.4.4.Responsabilidades.....	56
9.4.5.Prestación del consentimiento en el uso de los datos personales.....	56
9.4.6.Comunicación de la información a autoridades administrativas y/o judiciales.....	56
9.4.7.Otros supuestos de divulgación de la información.....	56
<b>9.5. DERECHOS DE PROPIEDAD INTELECTUAL .....</b>	<b>57</b>
<b>9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL.....</b>	<b>57</b>
9.6.1.Obligaciones de la Entidad de Certificación.....	57
9.6.2.Obligaciones de la Autoridad de Registro .....	59
9.6.3.Obligaciones de los suscriptores.....	60
9.6.4.Obligaciones de los terceros confiantes en los certificados emitidos por la ACEDICOM.....	61
9.6.5.Obligaciones del repositorio .....	61
<b>9.7. RENUNCIAS DE GARANTÍAS .....</b>	<b>61</b>
<b>9.8. LIMITACIONES DE RESPONSABILIDAD.....</b>	<b>62</b>
9.8.1.Garantías y limitaciones de garantías .....	62
9.8.2.Deslinde de responsabilidades.....	62
9.8.3.Limitaciones de pérdidas.....	62
<b>9.9. PLAZO Y FINALIZACIÓN. ....</b>	<b>62</b>
9.9.1.Plazo.....	62
9.9.2.Finalización.....	62
9.9.3.Supervivencia.....	62
<b>9.10.NOTIFICACIONES.....</b>	<b>63</b>
<b>9.11.MODIFICACIONES.....</b>	<b>63</b>
9.11.1.Procedimientos de especificación de cambios.....	63
9.11.2.Procedimientos de publicación y notificación.....	64
9.11.3.Procedimientos de aprobación de la Declaración de Prácticas de Certificación .....	64
<b>9.12.RESOLUCIÓN DE CONFLICTOS.....</b>	<b>64</b>
9.12.1.Resolución extrajudicial de conflictos.....	64
9.12.2.Jurisdicción competente.....	64

<b>9.13.LEGISLACIÓN APLICABLE .....</b>	<b>64</b>
<b>9.14.CONFORMIDAD CON LA LEY APLICABLE .....</b>	<b>64</b>
<b>9.15.CLÁUSULAS DIVERSAS.....</b>	<b>65</b>

## 1. INTRODUCCIÓN

### 1.1. PRESENTACIÓN

EDICOM se constituye en Prestador de Servicios de Certificación o Autoridad de Certificación en virtud del escrito remitido al Ministerio de Industria, Comercio y Turismo según lo dispuesto en La Ley 59/2003, de 19 de diciembre, de firma electrónica en su artículo 30, disposición transitoria segunda *“Los prestadores de servicios de certificación deberán comunicar al Ministerio de Industria, Turismo y Comercio el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen”*

EDICOM emite certificados ACEDICOM, que son **certificados reconocidos** de identificación y firma electrónica avanzada, destinados a personas físicas o a entidades jurídicas (colectivamente llamados suscriptores) que necesiten relacionarse con las Administraciones públicas y otras instituciones o empresas en el ámbito del Intercambio Electrónico de Datos y/o proveerse de sistemas de almacenamiento certificado.

El certificado ACEDICOM es un **certificado reconocido** de acuerdo con lo establecido en el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2, y emitido cumpliendo las obligaciones de los artículos 12, 13, 18 y 20 de la mencionada Ley.

Asimismo, los certificados cumplen los estándares en materia de certificados reconocidos, en concreto:

- ETSI TS 101 862: Qualified Certificate Profile.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

También emite la ACEDICOM certificados de servidor, y otros tipos de certificados para otros usos distintos de los de “firma electrónica”. No pueden considerarse sujetos a lo establecido en la Ley 59/2003 de Firma Electrónica, de 19 de Diciembre por no adecuarse al concepto legal de “certificado electrónico” definido por el artículo 6 de dicha ley, y no son aptos para dar soporte a la “Firma Electrónica” definida en la misma. Se citan en este documento exclusivamente porque forman parte del catálogo de certificados emitidos por la ACEDICOM pero no están sujetos a los criterios y procedimientos exigidos para los certificados reconocidos, aunque comparten toda la infraestructura física y de seguridad establecida para dichos certificados.

El presente documento se considera como la preceptiva *Declaración de Prácticas de Certificación (CPS)* de la Autoridad de Certificación EDICOM.

De acuerdo con lo anterior y en cumplimiento de la previsión legal contenida en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, la presente Declaración de Prácticas de Certificación (CPS) detalla las normas y condiciones generales de los servicios de certificación que presta la Autoridad de Certificación EDICOM, en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso, la existencia de procedimientos de coordinación con los registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

Así pues, la presente Declaración de Prácticas de Certificación constituye el compendio general de normas aplicables a toda actividad certificadora de la Autoridad de Certificación EDICOM en tanto que Prestador de Servicios de Certificación. Sin embargo, las distintas especialidades aplicables a cada uno de los diferentes tipos de certificados que se emitan se establecen en las distintas Políticas de Certificación que, como normas complementarias y específicas, prevalecerán sobre la presente Declaración de Prácticas de Certificación en lo que se refiera a cada tipo de certificado.

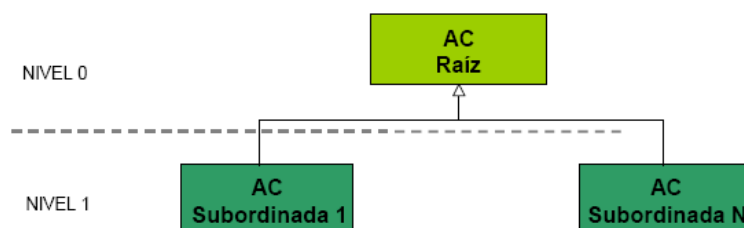
La presente Declaración de Prácticas de Certificación está redactada siguiendo las especificaciones del RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” propuesto por Network Working Group y completada con aspectos exigidos en:

- ETSI TS 101 456: “Policy Requirements for certification authorities issuing qualified certificates”.
- ETSI TS 101 862: “Qualified Certificate Profile”.
- ETSI TS 102 042: “Policy Requirements for certification authorities issuing public key certificates”.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

La arquitectura general, a nivel jerárquico, de la PKI EDICOM es la siguiente:



- Un primer nivel en el que se ubica la AC raíz que representa el punto de confianza de todo el sistema y que permitirá, tal y como recoge el artículo 15 de la Ley de Firma electrónica, que todas las personas físicas o jurídicas, públicas o privadas, reconozcan la eficacia de los certificados de EDICOM para firma electrónica.
- Un segundo nivel, constituido por las AC subordinadas de la AC Raíz que emitirán los certificados de identidad y firma de los suscriptores.

## 1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

<b>Nombre del documento</b>	Declaración de Prácticas de Certificación (CPS)
<b>Versión del documento</b>	1.4
<b>Estado del documento</b>	Vigente
<b>OID (Object Identifier)</b>	1.3.6.1.4.1.30051.2.1.1.1
<b>Fecha de emisión</b>	07 de Mayo de 2008
<b>Fecha de expiración</b>	No aplicable.
<b>Localización</b>	http://acedicom.edicomgroup.com

## 1.3. PARTICIPANTES DE LA PKI, COMUNIDAD DE USUARIOS CERTIFICADOS

Esta declaración de prácticas de certificación regula una comunidad de usuarios, que obtienen certificados para diversas relaciones administrativas y privadas, de acuerdo con la Ley 59/2003 y la normativa administrativa correspondiente.

### 1.3.1. Autoridades de Certificación

El prestador de servicios de certificación es EDICOM.

En la presente Declaración de Prácticas de Certificación, se utilizará el acrónimo "ACEDICOM" para designar en su conjunto a las Autoridades de Certificación que integran la ACEDICOM. Las funciones de la Autoridad de Certificación EDICOM están atribuidas al Departamento de Sistemas de EDICOM.

Las Autoridades de Certificación que componen ACEDICOM son:

- "ACEDICOM Root" como Autoridad de Certificación de primer nivel. Su función es la de establecer la raíz del modelo de confianza de la Infraestructura de Clave Pública o PKI. Esta AC no emite certificados para entidades finales. Esta Autoridad de Certificación de primer nivel se auto-firma. Sus datos más relevantes son:

Campo	Contenido	I	C	T
<b>Versión</b>	v3	S		F
<b>Serial Number</b>	61 8d c7 86 3b 01 82 05	S		F
<b>Signature Algorithm</b>	SHA1withRSAEncryption	S		F
<b>Issuer Distinguished Name</b>	CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES	S		F
<b>Validez</b>	7300 días	S		F
<b>Subject Public Key Info</b>	Tipo de clave: RSA Longitud de clave: 4096 bits	S		F
<b>Subject DN</b>		S		D
CommonName (CN)	ACEDICOM Root	S		D
Organizational Unit (OU)	PKI	O		D
Organization (O)	EDICOM	S		D
Country (C)	ES	S		D
<b>SubjectKeyIdentifier</b>	a6 b3 e1 2b 2b 49 b6 d7 73 a1 aa 94 f5 01 e7 73 65 4c ac 50	S		D
<b>AuthorityKeyIdentifier</b>	KeyId: (El mismo que SubjectKeyIdentifier porque el certificado es autofirmado)	S		F
<b>BasicConstraints</b>		S	X	F
CA	True	S	X	F
pathLength	-(Sin límite)	N		

<b>KeyUsage</b>	DigitalSignature, Certificate Sign, CRL Sign	S	X	F
<b>Certificate Policies</b>		S		F
policyIdentifier	2.5.29.32.0 (anyPolicy)	S		F
CPSuri	http://acedicom.edicomgroup.com	S		F
<b>CRLDistributionPoints</b>		S		F
distributionPoint	http://acedicom.edicomgroup.com/crlroot	S		F
<b>HUELLA DIGITAL</b>	e0 b4 32 2e b2 f6 a5 68 b6 54 53 84 48 18 4a 50 36 87 43 84	S		F

Leyenda empleada en las tablas:

I = Incluida. Posibles valores: S=Siempre, O=Opcionalmente, C=Condicionalmente

C = Crítica. Si se marca la casilla, indica que es crítica.

T = Tipo. Posibles valores: D = Dinámica, F = Fijada. Fijada quiere decir que el valor es el mismo para todos los certificados de este tipo.

- ACs subordinadas de ACEDICOM Root. Su función es la emisión de certificados de entidad final para los suscriptores de ACEDICOM. Sus datos más relevantes son:

#### ACEDICOM XX

Campo	Contenido	I	C	T
<b>Versión</b>	v3	S		F
<b>Serial Number</b>	Generado automáticamente por la CA	S		F
<b>Signature Algorithm</b>	SHA1withRSAEncryption	S		F
<b>Issuer Distinguished Name</b>	CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES	S		F
<b>Validez</b>	3650 días	S		F
<b>Subject Public Key Info</b>	Tipo de clave: RSA Longitud de clave: 4096 bits	S		F
<b>Subject DN</b>		S		D
CommonName (CN)	ACEDICOM XX	S		D
Organizational Unit (OU)	PKI	O		D
Organization (O)	EDICOM	S		D
Country (C)	ES	S		D
Location (L)	Ronda de Auguste y Louis Lumiere 12 Paterna			
Email (E)	acedicom@edicomgroup.com			
PostalCode	46980			
Número de serie	B96490867			
<b>SubjectKeyIdentifier</b>	Identificador de la clave pública del certificado	S		D
<b>AuthorityKeyIdentifier</b>	KeyId: a6 b3 e1 2b 2b 49 b6 d7 73 a1 aa 94 f5 01 e7 73 65 4c ac 50 Pertenece a ACEDICOM Root	S		F
<b>BasicConstraints</b>		S	X	F
CA	True	S	X	F
pathLength	- (Sin límite)	N		
<b>KeyUsage</b>	DigitalSignature, Certificate Sign, CRL Sign	S	X	F
<b>Certificate Policies</b>		S		F
policyIdentifier	1.3.6.1.4.1.30051.2.1.1.1	S		F
CPSuri	http://acedicom.edicomgroup.com	S		F
<b>CRLDistributionPoints</b>		S		F
distributionPoint	http://acedicom.edicomgroup.com/crl01	S		F
<b>Authority Information Access</b>		S		F
accessMethod	OCSP	S		F
AccessLocation	http://ocsp.edicomgroup.com	S		F

XX Es un número de dos dígitos que hace referencia a la AC emisora

### 1.3.2. Autoridades de Registro

Las Autoridades de Registro son aquellas personas físicas o jurídicas a las que la ACEDICOM encomienda la identificación y comprobación de las circunstancias personales de los solicitantes de certificados. A tal efecto, las Autoridades de Registro se encargarán de garantizar que la solicitud del certificado contiene información veraz y completa del Solicitante, y que la misma se ajusta a los requisitos exigidos en la correspondiente Política.

Pueden ser Autoridades de Registro tanto la empresa matriz EDICOM como las diferentes delegaciones de la misma que hayan sido autorizadas formalmente por ésta. Estas Autoridades de Registro, se designan Puntos de Registro de Usuario o PRUs en la documentación relativa a la Autoridad de Certificación EDICOM, y se les encomienda la confirmación de la identidad del solicitante y la entrega del certificado.

Las funciones de estas Autoridades de Registro, que actúan por cuenta de la ACEDICOM, se extienden a:

- Comprobar la identidad y cualesquiera circunstancias personales de los solicitantes de certificados relevantes para el fin propio de éstos.
- Informar con carácter previo a la emisión del certificado a la persona que lo solicite, de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso.
- Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

### 1.3.3. Usuarios finales

Las Entidades finales o Usuarios son las personas físicas o jurídicas que tienen capacidad para solicitar y obtener un certificado electrónico en las condiciones que se establecen en la presente Declaración de Prácticas de Certificación y en las Políticas de Certificación vigentes para cada tipo de certificado.

A los efectos de la presente Declaración de Prácticas de Certificación, y de las Políticas de Certificación que la desarrollan, son Entidades finales del sistema de certificación de la ACEDICOM, las siguientes:

- Solicitantes
- Suscriptores
- Terceros de confianza

#### 1.3.3.1. Solicitantes

*Solicitante* es la persona física que, en nombre propio o en representación de tercero, y previa identificación, solicita la emisión de un *Certificado*. En el supuesto de tratarse de un Solicitante de Certificado cuyo Suscriptor sea una persona jurídica dicha persona física sólo podrá ser un administrador o representante legal de la persona jurídica que vaya a ser el suscriptor del certificado o, en su caso, representante voluntario con poder notarial bastante que contenga una cláusula especial para solicitar el Certificado de Persona Jurídica a la ACEDICOM.

#### 1.3.3.2. Suscriptores

A los efectos de la presente CPS, el *suscriptor* de los certificados de ACEDICOM se corresponde con el término *firmante* previsto en el artículo 6 de la Ley 59/2003 de Firma Electrónica.

Tendrá la condición de suscriptor el titular del certificado. Es la persona física o jurídica cuya identidad personal queda vinculada a los datos de creación y verificación de firma, firmados electrónicamente, a través de una clave pública certificada por el Prestador de Servicios de Certificación.

El firmante asume la responsabilidad de custodia de los datos de creación de firma, sin que pueda ceder su uso a cualquier otra persona bajo ningún concepto.

El grupo de usuarios que pueden solicitar la emisión de certificados de ACEDICOM se encuentra definido y limitado por cada Política de Certificación.

De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, se establece que los posibles suscriptores son el conjunto de clientes de los servicios y aplicaciones de EDICOM.

#### 1.3.3.3. Partes confiantes

Tendrán la consideración de partes confiantes o terceras partes confiantes, todas aquellas personas que, de forma voluntaria, confían en los certificados emitidos por la ACEDICOM.

Las Políticas de Certificación aplicables en cada caso limitan el derecho a confiar en los certificados emitidos por ACEDICOM.

De forma genérica, y sin perjuicio de lo establecido por la Política de Certificación aplicable en cada caso, se establecen como terceros que confían en los certificados de ACEDICOM a los empleados, sistemas y aplicaciones de EDICOM.

## 1.4. USO DE LOS CERTIFICADOS

Esta sección lista las aplicaciones para las que puede utilizarse cada tipo de certificado, estableciendo limitaciones y prohíbe algunas aplicaciones de los certificados.

### 1.4.1 Usos típicos de los certificados

Las Políticas de Certificación correspondientes a cada tipo de certificado en concreto emitido por la ACEDICOM constituyen los documentos en los que se determinan los usos y limitaciones de cada certificado, aunque en este apartado se describe por su especial relevancia el uso principal de los certificados ACEDICOM reconocidos basados en dispositivos seguros de creación de firma.

El propósito principal de los certificados emitidos por la ACEDICOM es permitir al suscriptor firmar documentos. Este certificado (**certificado cualificado** según ETSI, la RFC3739 y la Directiva Europea 99/93/EC. y **reconocido** según la ley de Firma Electrónica) permite sustituir la firma manuscrita por la electrónica en las relaciones del suscriptor con terceros (LFE 59/2003 artº 3.4), asimismo también se emplearán para aportar seguridad en determinadas aplicaciones de almacenamiento certificado (“sustitutivo” en otras legislaciones)

Los certificados de firma expedidos por la ACEDICOM son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y se ajustan a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados emitidos por la ACEDICOM se expiden, cuando así se indica en las Políticas de Certificación propias del certificado, sobre dispositivo seguro de creación de firma, de acuerdo con el artículo 24.3, de la Ley 59/2003, de 19 de diciembre. Por este motivo, garantizan la identidad del suscriptor poseedor de la clave privada de identificación y firma, y permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma manuscrita para efectos legales, sin necesidad de cumplir ningún otro requerimiento adicional.

El uso de estos certificados proporcionan las siguientes garantías:

- No repudio de origen

Asegura que el documento proviene del suscriptor de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del **Certificado de Firma**. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando el servicio de validación de ACEDICOM. De esta forma garantiza que el documento proviene de un determinado suscriptor.

Dado que los certificados ACEDICOM son sobre dispositivos seguros de creación de firma y que las claves de firma permanecen desde el momento de su creación bajo el control del suscriptor titular, se garantiza el compromiso del mismo con la firma realizada (garantía de “no repudio”).

#### ▪ Integridad

Con el empleo del **Certificado de Firma**, se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de su resumen.

#### 1.4.2. Usos prohibidos

Los Certificados emitidos por ACEDICOM se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Declaración de Prácticas de Certificación y en las correspondientes Políticas de Certificación, y con arreglo a la normativa vigente.

La contratación de los certificados de la ACEDICOM admite solamente el uso del certificado en el ámbito de actividad del SOLICITANTE o de la entidad a la que está vinculado, de acuerdo con la finalidad del tipo de Certificado solicitado. Una vez emitido el Certificado, el SOLICITANTE no podrá, salvo acuerdo específico entre las partes, hacer uso con fines comerciales del mismo. Se entiende por uso comercial del certificado, cualquier actuación mediante la cual el SOLICITANTE ofrece a terceras partes ajenas al presente contrato, a título oneroso o gratuito, servicios que requieren el uso del certificado contratado.

En todo caso, los certificados ACEDICOM no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

#### 1.4.3. Fiabilidad de la firma electrónica a lo largo del tiempo

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

La generación de una firma longeva debe incluir los siguientes elementos:

**Sello de tiempo:** Se ha de incluir en la firma un sello de tiempo emitido por una Tercera Parte de Confianza, TSA (Autoridad de Sellado de Tiempo). El sello de tiempo asegura que tanto los datos originales del documento como la información del estado de los certificados, se generaron antes de una determinada fecha. El formato del sello de tiempo debe seguir el estándar definido en la RFC3161.

**Información de revocación:** La firma ha de incluir un elemento que asegura que el certificado de firma es válido. Este elemento será generado por una Tercera Parte de Confianza, en este caso por la ACEDICOM.

Es necesario que con posterioridad las firmas puedan renovarse (refirmado) y actualizar los elementos de confianza (sellos de tiempo) para dotar a las firmas electrónicas de validez a lo largo del tiempo, logrando garantizar su fiabilidad.

## 1.5. ADMINISTRACIÓN DE LAS POLÍTICAS

### 1.5.1. Organización responsable del CPS

<b>Nombre</b>	<i>Dirección Técnica de EDICOM</i>
<b>Dirección de email</b>	<i>acedicom@edicomgroup.com</i>
<b>Dirección</b>	<i>C/ Auguste y Louis Lumiere, 12B – Parque Tecnológico, 46980 Paterna (Valencia) ESPAÑA</i>
<b>Número de teléfono</b>	<i>+34-902 119 229</i>
<b>Número de fax</b>	<i>+34-96 348 16 88</i>

### 1.5.2. Persona de Contacto para el CPS

<b>Nombre</b>	<i>Departamento sistemas EDICOM</i>
<b>Dirección de email</b>	<i>acedicom@edicomgroup.com</i>
<b>Dirección</b>	<i>C/ Auguste y Louis Lumiere, 12B – Parque Tecnológico, 46980 Paterna (Valencia) ESPAÑA</i>
<b>Número de teléfono</b>	<i>+34-902 119 229</i>
<b>Número de fax</b>	<i>+34-96 348 16 88</i>

### 1.5.3. Competencia para determinar la adecuación de la CPS con las diferentes Políticas de certificación.

La Dirección Técnica de EDICOM es el órgano competente para determinar la adecuación de esta CPS a las distintas Políticas de Certificación de la Autoridad de Certificación de EDICOM.

### 1.5.4 Procedimiento de aprobación

El sistema documental y de organización de ACEDICOM garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de la Declaración de prácticas de certificación y de las especificaciones de servicio relacionadas con ella.

Se prevé, de esta manera, el procedimiento de modificación de especificación del servicio y el procedimiento de publicación de especificaciones de servicio.

Las modificaciones finales de la política son aprobadas por ACEDICOM, después de comprobar el cumplimiento de los requisitos establecidos en las secciones correspondientes de esta CPS.

## 1.6. DEFINICIONES Y ACRÓNIMOS

### 1.6.1. Definiciones

A los efectos de determinar el alcance de los conceptos que son utilizados en la presente Declaración de Prácticas de Certificación, y en las distintas Políticas de Certificación, deberá entenderse:

- *Autoridad de Certificación*: es aquella persona física o jurídica que, de conformidad con la legislación sobre firma electrónica expide certificados electrónicos, pudiendo prestar además otros servicios en relación con la firma electrónica. A efectos de la presente Declaración de Prácticas de Certificación, son Autoridad de Certificación todas aquellas que en la misma se definan como tales.

- **Autoridad de Registro:** persona física o jurídica que ACEDICOM designa para realizar la comprobación de la identidad de los solicitantes y suscriptores de certificados, y en su caso de la vigencia de facultades de representantes y subsistencia de la personalidad jurídica o de la representación voluntaria. En la ACEDICOM reciben también el nombre de PRU's o Puntos de Registro del Usuario.
- **Cadena de certificación:** lista de certificados que contiene al menos un certificado y el certificado raíz de ACEDICOM.
- **Certificado:** documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula al suscriptor unos datos de verificación de firma y confirma su identidad. En la presente Declaración de Prácticas de Certificación, cuando se haga referencia a certificado se entenderá realizada a un Certificado emitido por ACEDICOM.
- **Certificado raíz:** Certificado cuyo suscriptor es ACEDICOM y pertenece a la jerarquía de ACEDICOM como Prestador de Servicios de Certificación, y que contiene los datos de verificación de firma de dicha Autoridad firmado con los datos de creación de firma de la misma como Prestador de Servicios de Certificación.
- **Certificado reconocido:** Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica .
- **Clave:** secuencia de símbolos.
- **Datos de creación de Firma (Clave Privada):** son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la Firma electrónica.
- **Datos de verificación de Firma (Clave Pública):** son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma electrónica.
- **Declaración de Prácticas de Certificación:** declaración de ACEDICOM puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de Prestador de Servicios de Certificación en cumplimiento de lo dispuesto por la Ley.
- **Dispositivo seguro de creación de Firma:** instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- **Directorio de Certificados:** repositorio de información que sigue el estándar X.500 del ITU-T.
- **Documento electrónico:** conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.
- **Documento de seguridad:** documento exigido por la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por ACEDICOM como Prestador de Servicios de Certificación, para la protección de los datos de carácter personal contenidos en los Ficheros de la actividad de certificación que contienen datos personales (en adelante los Ficheros).
- **Encargado del Tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento de los ficheros.
- **Firma electrónica reconocida:** es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- **Firma electrónica avanzada:** es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.
- **Firma electrónica:** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.
- **Función hash:** es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado

unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

- *Hash o Huella digital*: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
- *Infraestructura de Claves Públicas (PKI, public key infrastructure)*: infraestructura que soporta la emisión y gestión de claves y certificados para los servicios de autenticación, cifrado, integridad, o no repudio.
- *Listas de Revocación de Certificados o Listas de Certificados Revocados*: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).
- *Módulo Criptográfico Hardware de Seguridad*: módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.
- *Número de serie de Certificado*: valor entero y único que está asociado inequívocamente con un certificado expedido por ACEDICOM.
- *OCSP (Online Certificate Status Protocol)*: protocolo informático que permite la comprobación del estado de un certificado en el momento en que éste es utilizado.
- *OCSP Responder*: servidor informático que responde, siguiendo el protocolo OCSP, a las peticiones OCSP con el estado del certificado por el que se consulta.
- *OID (Object Identifier)*: valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID.
- *Petición OCSP*: petición de consulta de estado de un certificado a OCSP Responder siguiendo el protocolo OCSP.
- *PIN: (Personal Identification Number)* número específico sólo conocido por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- *Prestador de Servicios de Certificación*: es aquella persona física o jurídica que, de conformidad con la legislación sobre firma electrónica expide certificados electrónicos, pudiendo prestar además otros servicios en relación con la firma electrónica. En la presente Declaración de Prácticas de Certificación, se corresponderá con las Autoridades de Certificación pertenecientes a la jerarquía de ACEDICOM.
- *Política de Certificación*: documento que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por ACEDICOM para emitir Certificados.
- *PKCS#10 (Certification Request Syntax Standard)*: estándar desarrollado por RSA Labs, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de certificado.
- *PUK: (Personal Unblocking Key)* número o clave específica sólo conocido por la persona que tiene que acceder a un recurso que se utiliza para desbloquear el acceso a dicho recurso.
- *Recertificación*: Revocación de un certificado de usuario para a continuación proporcionar al usuario la emisión de un nuevo certificado de las mismas características del revocado, no necesariamente firmado con la misma CA que emitió el certificado revocado.
- *Responsable del Fichero (o del Tratamiento del Fichero)*: persona que decide sobre la finalidad, contenido y uso del tratamiento de los Ficheros.
- *Responsable de Seguridad*: encargado de coordinar y controlar las medidas que impone el documento de seguridad en cuanto a los ficheros.
- *SHA-1: Secure Hash Algorithm* (algoritmo seguro de resumen –hash–). Desarrollado por el NIST y revisado en 1994 (SHA-1). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma electrónica.
- *Sellado de Tiempo*: constatación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones Request For

Comments: 3161 – “Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP)”, que logra datar el documento de forma objetiva.

- *Solicitante*: persona física que previa identificación, solicita la emisión de un certificado.
- *Suscriptor (o Subject)*: el titular o firmante del certificado. La persona cuya identidad personal queda vinculada a los datos firmados electrónicamente, a través de una clave pública certificada por el Prestador de Servicios de Certificación. El concepto de suscriptor, será referido en los certificados y en las aplicaciones informáticas relacionadas con su emisión como Subject, por estrictas razones de estandarización internacional.
- *Tarjeta criptográfica*: tarjeta utilizada por el suscriptor para almacenar claves privadas de firma y descifrado, para generar firmas electrónicas y descifrar mensajes de datos. Tiene la consideración de dispositivo seguro de creación de firma de acuerdo con la Ley y permite la generación de firma electrónica reconocida.
- *Terceras partes confiantes o partes confiantes*: aquellas personas que depositan su confianza en un certificado de ACEDICOM, comprobando la validez y vigencia del certificado según lo descrito en esta Declaración de Prácticas de Certificación y en las Políticas de Certificación asociadas a cada tipo de certificado.
- *X.500*: estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525.
- *X.509*: estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.

## 1.6.2.Acrónimos

<i>ACEDICOM</i>	Autoridad de Certificación EDICOM
<i>CA</i>	Certification Authority
<i>CP</i>	Certificate Policy
<i>CPS</i>	Certification Practice Statement
<i>CRL</i>	Certificate Revocation List
<i>FIPS</i>	<i>Federal Information Processing Standards</i>
<i>IETF</i>	Internet Engineering Task Force
<i>OID</i>	Object identifier
<i>OCSP</i>	On-line Certificate Status Protocol
<i>OPRU</i>	Operador de Punto de Registro
<i>PKI</i>	Public Key Infrastructure
<i>PKIEDICOM</i>	PKI de EDICOM
<i>PRU</i>	Punto de Registro de usuarios
<i>RA</i>	Registration Authority
<i>RFC</i>	Request For Comment
<i>Sub CA</i>	Subordinate Certification Authority

## 2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

### 2.1. REPOSITORIOS

El servicio de repositorio de la ACEDICOM estará disponible durante las 24 horas del día, los 7 días de la semana, y en caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en el menor tiempo posible.

Entendiendo por disponibilidad, la capacidad de acceder al servicio por parte de quien lo demanda, con independencia de la rapidez o ritmo al que posteriormente éste sea prestado.

En ningún caso esta disponibilidad, podrá ser inferior a un **99,5%** en tiempo primario (Lunes a Sabado de 08:00 a 00:00 horas y de 00:00 a 02:00) y de un **99%** el resto del tiempo, medido en el periodo de un mes.

EDICOM se reserva hasta un máximo de 1 hora diaria fuera del horario primario de Lunes a Viernes y hasta 3 Horas los Sábados y Domingos alternos y en el momento de mínima actividad, para efectuar tareas de mantenimiento, backups del sistema, etc.

Este tiempo quedará excluido a efecto de los cálculos de nivel de servicio.

Si existe un mal funcionamiento de los sistemas que operan los Servicios, EDICOM informará al Cliente tan pronto como razonablemente pueda sobre el problema y el tiempo previsto para el suministro normal. EDICOM proporcionará al Cliente recursos del centro de atención a usuarios y hará todo lo posible para rectificar el problema en el menor tiempo posible.

En caso de desastres, se mantendrá un plan completo de recuperación del desastre y se invocará si se espera que la interrupción del servicio dure más de 48 horas. EDICOM mantendrá el plan actualizado en la línea de la mejor práctica de la empresa

El repositorio de ACEDICOM no contiene ninguna información de naturaleza confidencial.

ACEDICOM no utiliza ningún otro repositorio operado por ninguna organización distinta a ACEDICOM.

### 2.2. PUBLICACIÓN

Es obligación de las ACs pertenecientes a la jerarquía de confianza de ACEDICOM publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados.

La presente CPS es pública y se encuentra disponible en el sitio web de ACEDICOM <http://acedicom.edicomgroup.com>, en formato PDF.

Las Políticas de Certificación de ACEDICOM son públicas y se encuentran disponibles en el sitio de web de ACEDICOM <http://acedicom.edicomgroup.com>, en formato PDF.

El certificado de la AC de ACEDICOM es público y se encuentra disponible en el repositorio de ACEDICOM, en formato X.509 v3. También se encuentra en la <http://acedicom.edicomgroup.com>.

La lista de certificados revocados por ACEDICOM es pública y se encuentra disponible, en formato CRL v2. También se encuentra en la <http://acedicom.edicomgroup.com>

### 2.3. FRECUENCIA DE ACTUALIZACIONES

La CPS y las Políticas de Certificación se publicarán cada vez que sean modificadas.

La AC añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto 4.9.9 *Frecuencia de emisión de CRLs*.

### 2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.

El acceso a lectura de la información del repositorio de ACEDICOM y de su sitio web es libre.

Sólo ACEDICOM está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. En este sentido, la ACEDICOM utiliza los medios de control adecuados a fin de restringir la capacidad de escritura o modificación de estos elementos.

## 3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE LOS CERTIFICADOS

### 3.1. REGISTRO DE NOMBRES

En esta sección se establecen requisitos relativos a los procedimientos de identificación y autenticación que se utilizan durante el registro de Entidades de Certificación Vinculadas (si las hubieren) y suscriptores, que tiene que realizarse con anterioridad a la emisión y entrega de certificados.

#### 3.1.1. Tipos de nombres

El campo *Subject DN (Distinguished Name)* contiene toda la información de identificación de la entidad para la que se emite el certificado, ya sea persona jurídica, física, o cualquier otro tipo. Dicha información debe identificar unívocamente a un certificado emitido por una misma CA, es decir: no deben existir dos certificados emitidos por una misma CA cuyo *Subject* sea idéntico.

Es muy importante en el caso de los certificados reconocidos (*Qualified Certificates*) tener en cuenta que el contenido de *commonName (CN)* debe ser un nombre válido del sujeto del certificado. Sólo se considerará como válido el nombre y apellidos no permitiendo el uso de seudónimos.

Además, hay que tener en cuenta que muchas implementaciones presuponen la presencia del atributo *commonName*, y emplean su contenido para mostrar el nombre del sujeto, independientemente de otros atributos tales como *givenName*, *surname*, o *pseudonym*.

Además los certificados reconocidos (*Qualified Certificates*) deben siempre ser emitidos a personas físicas, como se indica en el estándar ETSI TS 101 862 (*Qualified Certificate Profile*) y en la RFC 3739, sección 2.1.

Todos los atributos siguientes han de aparecer, a no ser que se dependa de algún factor (indicando "si procede"). Por ejemplo, si una persona en lugar de representar a una empresa es autónomo, en dicho caso no procedería emplear los atributos O, OU, etc.

<b>CN</b>	Nombre y apellidos
<b>SN (Serial Number)</b>	NIF
<b>GN</b>	Nombre de pila
<b>S</b>	Apellidos
<b>T</b>	Puesto que ocupa en la organización a la que pertenece (si procede) Identificador del Distinguished Name. Forzado por la legislación italiana.
<b>DN Qualifier</b>	Es un identificador que da el emisor del certificado para identificar de manera unívoca al sujeto del mismo. Se pondrá el NIF.
<b>OU</b>	Departamento de la empresa/organización a la que pertenece (si procede)
<b>O</b>	Empresa/organización a la que pertenece (si procede)
<b>C</b>	Código ISO de país (ES, FR, IT, MX, etc)
<b>OID</b> <b>1.3.6.1.4.1.30051.3.1.1</b>	CIF de la organización a la que representa el sujeto (si procede)

#### 3.1.2. Significado de los nombres

Las reglas definidas en el apartado anterior, garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con una identidad..

### 3.1.3. Interpretación de formatos de nombres

Las reglas utilizadas por ACEDICOM para interpretar los nombres distintivos de los certificados que emite son las contenidas en la ISO/IEC 9595 (X.500) Distinguished Name (DN)

### 3.1.4. Unicidad de los nombres

Los nombres distintivos deben ser únicos y no inducirán a ambigüedad.

El DN de los certificados no puede estar repetido. La utilización del número del CIF de la empresa y del NIF del solicitante garantiza la unicidad del DN.

Las Políticas de Certificación pueden disponer la sustitución de este mecanismo de unicidad.

### 3.1.5. Resolución de conflictos relativos a nombres

La inclusión en un certificado de un nombre no implica la existencia de ningún derecho sobre el mismo y lo es sin perjuicio del mejor derecho que pudieren ostentar terceros.

La ACEDICOM no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc.

La ACEDICOM se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto sobre el nombre.

### 3.1.6. Reconocimiento, autenticación y función de las marcas registradas.

No estipulado.

## 3.2. VALIDACIÓN DE LA IDENTIDAD INICIAL

### 3.2.1. Métodos de prueba de posesión de la clave privada.

Habrà que atenerse a lo establecido en cada caso en la Política de Certificación aplicable para cada solicitud.

### 3.2.2. Autenticación de la identidad de una organización.

La autenticación de la identidad de una organización o entidad se realizará mediante la presentación ante el Operador del Punto de Registro habilitado para la emisión de este tipo de certificados por parte del solicitante del certificado de entidad (administrador, representante legal o representante voluntario con poder bastante) una vez acreditada su identidad tal como se define en el punto 3.2.3, de la documentación que se establece en el párrafo cuarto de este punto, y la extensión y vigencia de sus facultades de representación sobre esa entidad.

El Operador del Punto de Registro de ACEDICOM comprobará los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación o representación voluntaria del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, se exigirá la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente. Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

La documentación que se requiere para realizar las comprobaciones varía en función del tipo de entidad para la que se solicite el certificado. Por ello, y con carácter general, se aportará la siguiente documentación:

- Para solicitar certificado electrónico de una sociedad mercantil o cualquier sociedad de inscripción obligatoria en el Registro Mercantil (Sociedad Anónima, Sociedad de Responsabilidad Limitada, Sociedad Laboral, Sociedad Deportiva, Sociedades Colectivas, Comanditarias o Cooperativas, Agrupaciones de Interés Económico, UTE, otras..), se deberá aportar certificado del Registro Mercantil relativo a la constitución, personalidad jurídica y nombramiento y vigencia del cargo de administrador o representante legal, expedido durante los 10 días anteriores a la fecha de presentación del certificado en la ACEDICOM. Si la representación es voluntaria, se sustituirá el certificado de nombramiento y vigencia del cargo por el poder notarial bastante, con la cláusula especial para poder solicitar el Certificado de Persona Jurídica.
- Para solicitar un certificado de Asociaciones, Fundaciones, Clubes, Partidos Políticos, Sindicatos o Cooperativas no inscribibles en el Registro Mercantil, se aportará certificado del registro público donde consten inscritas, relativo a la constitución, personalidad jurídica y nombramiento y vigencia del cargo de administrador o representante legal, expedido durante los 10 días anteriores a la fecha de presentación del certificado en la ACEDICOM. Si la representación es voluntaria, se sustituirá el certificado de nombramiento y vigencia del cargo por el poder notarial bastante, con la cláusula especial para poder solicitar el Certificado de Persona Jurídica.
- Para solicitar un certificado electrónico de Sociedades Civiles y Comunidades de Bienes, se aportará el Título Constitutivo de la Sociedad Civil o Estatutos, el NIF, el certificado del nombramiento del Presidente u órgano de administración y la manifestación responsable del Presidente (u órgano de administración) sobre la vigencia de su cargo, o bien poder notarial bastante con cláusula especial para la solicitud del certificado de persona jurídica, otorgado por el Presidente u órgano de administración al representante voluntario.
- En todos los casos el solicitante deberá acompañar la documentación del "CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL" que podrá descargarse en el sitio web de ACEDICOM <http://acedicom.edicomgroup.com>

La ACEDICOM guardará copia de la documentación presentada por el solicitante.

Efectuadas todas estas comprobaciones se crea una solicitud de expedición del certificado en el sistema informático enviándolo electrónicamente y de forma segura a la ACEDICOM.

En el caso que una Política de Certificación considere necesaria otro procedimiento de autenticación de la identidad de una organización, dicha política será la responsable del establecimiento de los métodos necesarios para la verificación de la mencionada identidad.

Se admitirá como medio de autenticación indirecto aquel que se base en documentación de registro que haya tenido que presentarse necesariamente por medios presenciales (TS 101 456).

### 3.2.3. Autenticación de la identidad de un individuo.

El proceso de identificación individual se define por la Política de Certificación aplicable a cada tipo de certificado, como norma general podrá emplearse para este fin indistintamente la personación física ante el Operador del Punto de Registro o bien la identificación remota.

Cuando la autenticación de la identidad del solicitante de un certificado se realice mediante su personación ante el Operador del Punto de Registro, se acreditará mediante la presentación de un documento oficial de identidad válido y en vigor como Documento Nacional de Identidad, pasaporte, o el Número de Identificación de Extranjeros (NIE) del solicitante y se comprobará explícitamente la fecha y el lugar de nacimiento.

Cuando la autenticación se realice de forma remota, en general no se emplearán métodos de identificación distintos a la firma digital realizada con certificados emitidos por la propia ACEDICOM o por algún otro Prestador de Servicios de Certificación que expida certificados reconocidos.

También se podrá prescindir de la presencia física si la firma contenida en la solicitud de expedición de un certificado ha sido legitimada notarialmente, y en los casos previstos por el artículo 13.4 de la Ley 59/2003, de 19 de diciembre.

## 3.3. IDENTIFICACION Y AUTENTICACION DE LAS SOLICITUDES DE RENOVACION DE CLAVE.

### 3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se puede realizar utilizando las técnicas para la autenticación e identificación inicial o utilizando solicitudes firmadas digitalmente mediante el certificado original que se pretende renovar, siempre que este no haya vencido ni se haya procedido a su revocación. Existen, por tanto, dos mecanismos alternativos para la renovación:

- Formularios web firmados en el Área “Gestión de Certificados” disponible en <http://acedicom.edicomgroup.com>
- Personación en cualquier Punto de Registro de Usuario, con los documentos de identificación suficientes (ver apartado 3.2.2 y 3.2.3 de esta CPS).

Asimismo, y de conformidad con lo establecido en el art. 13.4 b) de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica la renovación del certificado mediante solicitudes firmadas digitalmente exigirá que haya transcurrido un período de tiempo desde la identificación personal menor a los cinco años.

### 3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial, tal como se describe en este mismo documento en el punto 3.2.3. de forma que se garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

## 3.4. IDENTIFICACION Y AUTENTICACION DE LAS SOLICITUDES DE REVOCACION DE LA CLAVE

El proceso de solicitud de revocación viene definido por la Política de Certificación aplicable a cada tipo de certificado. La política de identificación para las solicitudes de revocación podrá ser la

misma que para el registro inicial. La política de autenticación aceptará solicitudes de revocación firmadas digitalmente por el suscriptor del certificado.

ACEDICOM o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del suscriptor, o cualquier otro hecho que recomendará emprender dicha acción.

El procedimiento general de revocación se describe en esta Política en el punto 4.9.3. En cualquier caso, las distintas Políticas de Certificación pueden definir otras políticas de identificación menos severas así como también pueden definir la creación de una contraseña de revocación en el momento del registro del certificado.

## 4. EL CICLO DE VIDA DE LOS CERTIFICADOS.

Las especificaciones contenidas en este apartado lo son sin perjuicio de las estipulaciones previstas en cada una de las distintas Políticas de Certificación para los distintos tipos de certificados emitidos por la ACEDICOM.

### 4.1. SOLICITUD DE CERTIFICADOS

La Autoridad de Registro de la ACEDICOM que reciba la solicitud le compete el determinar que el tipo de certificado solicitado se adecue a las características concretas del solicitante, de conformidad con el contenido de la Política de Certificación aplicable a dicho certificado y, de este modo, resolver la solicitud formulada.

En cada Política de Certificación se especifica la información que debe suministrarse con carácter previo, a quien solicite un certificado.

### 4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.

Compete a la Autoridad o Entidad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado el documento de comparecencia (CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL). Una vez completa la solicitud y efectuadas las comprobaciones pertinentes, la Autoridad de Registro procederá a efectuar la solicitud de emisión a la Autoridad de Certificación de la ACEDICOM y a almacenar copia de la solicitud y de la documentación asociada.

### 4.3. EMISIÓN DE CERTIFICADOS

ACEDICOM no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

La emisión del certificado tendrá lugar una vez que ACEDICOM haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación. El mecanismo por el que determina la naturaleza y la forma de realizar dichas comprobaciones es la Política de Certificación.

Cuando la ACEDICOM emita un certificado de acuerdo con una solicitud de certificación válida, notificará a la Entidad de Registro que remitió la solicitud y guardará el mismo en el repositorio de ACEDICOM.

La ACEDICOM:

- a. Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada
- b. Protege la confidencialidad e integridad de los datos de registro
- c. Toma medidas contra la falsificación de certificados.

Es tarea de la Entidad de Registro notificar al suscriptor de un certificado la emisión del mismo y proporcionarle los datos de acceso al mismo.

Todo lo especificado en este apartado queda supeditado a lo estipulado por las distintas Políticas de Certificación para la emisión de cada tipo de certificados.

### 4.4. ACEPTACIÓN DE CERTIFICADOS

La aceptación de los certificados por parte de los firmantes se produce en el momento de la firma del "CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL" asociado a cada Política de Certificación. La aceptación del contrato implica el conocimiento y aceptación por parte del suscriptor de la Política de Certificación asociada.

#### 4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.

Los certificados ACEDICOM, según se estipula en sus políticas específicas, son certificados de identificación y firma electrónica avanzada, destinados a personas físicas o a entidades jurídicas (colectivamente llamados suscriptores) que necesiten relacionarse con las Administraciones públicas y otras instituciones o empresas en el ámbito del Intercambio Electrónico de Datos y/o proveerse de sistemas de almacenamiento certificado.

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece esta CPS y de acuerdo con lo establecido en el campo 'Key Usage' del certificado.

En todo caso, los certificados ACEDICOM no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

#### 4.6. RENOVACIÓN DE CERTIFICADOS

El periodo de renovación del certificado se debe iniciar 70 días antes de la fecha de caducidad del certificado. Estos pasos se explican el apartado 3.3

#### 4.7. RENOVACIÓN DE CLAVES

La renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

#### 4.8. MODIFICACIÓN DE CERTIFICADOS.

Todas las circunstancias que obligarían a efectuar modificaciones en los certificados emitidos a un suscriptor por variación de los datos contenidos en el mismo, también obligarían al cambio del soporte físico por lo se tratarán como una renovación del soporte por variación de datos, siendo de aplicación los apartados anteriores.

#### 4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.

Seguidamente se informa de aspectos a tener en cuenta para la revocación y suspensión de certificados.

##### 4.9.1. Circunstancias para la revocación

Un certificado se revoca cuando:

- El suscriptor del certificado o sus claves o las claves de sus certificados se han comprometido por:
  - El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del usuario.
  - El mal uso deliberado de claves y certificados, o la falta de observación de los requerimientos operacionales del acuerdo de suscripción, la CP asociada o de la presente CPS.
- Se produce la emisión defectuosa de un certificado debido a:
  - Que no se ha satisfecho un prerequisite material para la emisión del certificado.
  - Que un factor fundamental en el certificado se sepa o crea razonablemente que puede ser falso.
  - Un error de entrada de datos u otro error de proceso.
- La información contenida en un certificado o utilizada para realizar su solicitud se convierte en inexacta, por ejemplo cuando el dueño de un certificado cambia su nombre.

- Una solicitud de revocación válida se recibe de un usuario final.
- Una solicitud de revocación válida se recibe de una tercera parte autorizada, por ejemplo una orden judicial.
- El certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado.
- Cese en la actividad del prestador de servicios de certificación

#### 4.9.2. Entidad que puede solicitar la revocación

La revocación de un certificado se puede instar tanto por el suscriptor del mismo como por parte de ACEDICOM.

Los suscriptores de certificados pueden solicitar su revocación por cualquier causa y deben solicitarla bajo las condiciones especificadas en el siguiente apartado.

#### 4.9.3. Procedimiento de solicitud de revocación

El procedimiento para la solicitud de la revocación de cada tipo de certificado se definirá en la Política de Certificación correspondiente.

De forma general, y sin perjuicio de lo definido en las Políticas de Certificación:

- Se aceptarán solicitudes de revocación remotas si están firmadas digitalmente con un certificado de ACEDICOM o de algún otro Prestador de Servicios de Certificación que expida Certificados Reconocidos, y presencial si se cumplen los requisitos de identificación del usuario establecidos para el registro inicial.
- Tras la revocación del certificado el suscriptor del mismo deberá destruir la clave privada que se corresponda con el mismo, y no hacer uso del certificado revocado.

Existe un formulario de solicitud de revocación de certificados en la web de ACEDICOM <http://acedicom.edicomgroup.com>

Una solicitud de revocación tanto si se realiza en papel o de forma electrónica debe contener la información que se describe en el formulario de solicitud de revocación, recogido en cada una de las Políticas de Certificación. No obstante ACEDICOM se compromete a publicar inmediatamente mediante OCSP el nuevo estado del certificado en cuanto se constaten los motivos de la revocación solicitada. Así mismo, el certificado será incluido en las listas CRL publicadas por ACEDICOM en el próximo ciclo de renovación de CRL, cuya periodicidad es de 24 horas.

Se informará a los suscriptores de los cambios de estado en sus certificados a través de un correo electrónico.

#### 4.9.4. Periodo de gracia de la solicitud de revocación

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida. Por tanto no existe ningún periodo de gracia asociado a este proceso.

#### 4.9.5. Circunstancias para la suspensión

No se contempla

#### 4.9.6. Entidad que puede solicitar la suspensión

No se contempla

#### 4.9.7. Procedimiento para la solicitud de suspensión

No se contempla

#### 4.9.8. Límites del período de suspensión

No se contempla

#### 4.9.9.Frecuencia de emisión de CRLs

ACEDICOM publicará una nueva CRL en su repositorio en intervalos de máximo 24 horas, aunque no se hayan producido modificaciones en la misma (cambios de estado de certificados) durante el citado periodo. Este periodo tampoco se ve afectado en caso de revocaciones de certificados, que ya obtienen respuesta inmediata en la publicación mediante OCSP.

Las CRLs se generan y se firman con la clave de la CA.

#### 4.9.10.Requisitos de comprobación de CRLs

La verificación de las revocaciones es obligatoria para cada uso de los certificados de identidad pública. El procedimiento ordinario de comprobación de la validez de un certificado será la consulta a los Servicios de Validación de ACEDICOM, los cuales mediante protocolo OCSP indicarán el estado del certificado.

También contempla la ACEDICOM la publicación de CRLs.

Se informará a los suscriptores de los cambios de estado en sus certificados a través de un correo electrónico.

#### 4.9.11.Otras formas de información de los certificados revocados

La ACEDICOM puede establecer en el futuro otras formas para informar sobre la revocación de los certificados.

#### 4.9.12.Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

### 4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.

#### 4.10.1. Características operativas

Para la validación de certificados la ACEDICOM dispone de Servicios de Validación en línea, además de la publicación de CRLs, que proporcionan información sobre el estado de los certificados emitidos por la jerarquía de certificación del ACEDICOM. Se trata de un servicio de validación en línea (Autoridad de Validación, AV) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560. Mediante el uso de ese protocolo se determina el estado actual de un certificado electrónico sin requerir las CRLs. Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su BBDD, ofrece una respuesta sobre el estado del certificado vía HTTP.

Para hacer uso del Servicio de validación en línea es responsabilidad del Tercero Aceptante disponer de un Cliente OCSP que cumpla la RFC 2560.

#### 4.10.2. Disponibilidad del servicio

Los sistemas CRLs y de consulta en línea del estado de los certificados están disponibles durante las 24 horas los 7 días de la semana.

Entendiendo por disponibilidad, la capacidad de acceder al servicio por parte de quien lo demanda, con independencia de la rapidez o ritmo al que posteriormente éste sea prestado.

En ningún caso esta disponibilidad, podrá ser inferior a un **99,5%** en tiempo primario (Lunes a Sabado de 08:00 a 00:00 horas y de 00:00 a 02:00) y de un **99%** el resto del tiempo, medido en el periodo de un mes.

EDICOM se reserva hasta un máximo de 1 hora diaria fuera del horario primario de Lunes a Viernes y hasta 3 Horas los Sábados y Domingos alternos y en el momento de mínima actividad, para efectuar tareas de mantenimiento, backups del sistema,etc.

Este tiempo quedará excluido a efecto de los cálculos de nivel de servicio.

Si existe un mal funcionamiento de los sistemas que operan los Servicios, EDICOM informará al Cliente tan pronto como razonablemente pueda sobre el problema y el tiempo previsto para el suministro normal. EDICOM proporcionará al Cliente recursos del centro de atención a usuarios y hará todo lo posible para rectificar el problema en el menor tiempo posible.

En caso de desastres, se mantendrá un plan completo de recuperación del desastre y se invocará si se espera que la interrupción del servicio dure más de 48 horas. EDICOM mantendrá el plan actualizado en la línea de la mejor práctica de la empresa

#### 4.11.FINALIZACIÓN DE LA SUSCRIPCIÓN.

La suscripción finaliza con la expiración o revocación del certificado.

#### 4.12.DEPÓSITO Y RECUPERACIÓN DE CLAVES.

La ACEDICOM puede emitir en función de su soporte certificados reconocidos de dos tipos:

Sobre dispositivo seguro o de Software. Únicamente para el primer caso, el hardware soporte de los certificados emitidos por ACEDICOM está certificado CWA14169. Los datos de creación de firma (las claves privadas) se generan dentro del hardware y no pueden ser exportadas en ningún caso. Sólo en el caso de dispositivo SSCD centralizado se hace el depósito de las claves privadas por parte de la ACEDICOM pero sólo tiene acceso a las mismas el propio usuario mediante los correspondientes datos de activación que sólo él conoce.

Los detalles particulares se recogen en las Políticas de Certificación asociadas a cada tipo de certificado.

## 5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

### 5.1. CONTROLES DE SEGURIDAD FÍSICA

La ACEDICOM ofrece a sus suscriptores el más alto nivel de seguridad física para la realización de las tareas imprescindibles en la generación y gestión de los certificados.

De esta forma dispone de instalaciones con diversos perímetros de seguridad alrededor de los servicios de generación de certificados, de los dispositivos criptográficos y de la gestión de revocación.

Así la ACEDICOM controla la seguridad física y ambiental de las instalaciones y los sistemas que se encuentran en dichas instalaciones, con las siguientes medidas:

- Controles de acceso físico
- Protección ante desastres naturales
- Medidas de protección ante incendios
- Fallo de los sistemas de soporte (energía eléctrica, telecomunicaciones, etc)
- Inundaciones
- Protección antirrobo
- Conformidad y entrada no autorizada
- Recuperación del desastre
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativas a componentes utilizados para los servicios de la ACEDICOM.

#### 5.1.1. Ubicación y construcción

Los sistemas de información de la ACEDICOM se ubican en Centros de Proceso de Datos con unos niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

#### 5.1.2. Acceso físico

Los Centros de Proceso de Datos de la ACEDICOM disponen de diversos perímetros de seguridad, con diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico por combinación y biométricos, sistemas de videovigilancia y de grabación, de detección de intrusiones entre otros.

#### 5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los periodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El apagado de los equipos sólo se producirá en caso de fallo de los sistemas de generación autónoma de alimentación.

El sistema de acondicionamiento ambiental está compuesto por varios equipos independientes con capacidad para mantener niveles de temperatura dentro de los márgenes de operación óptimos de los sistemas.

#### 5.1.4. Exposición al agua

La ubicación actual y el diseño de la sala informática de la ACEDICOM garantiza la inexistencia de peligro por inundación, aunque se han diseñado los procedimientos necesarios para poder detectar presencia de agua en la sala.

### 5.1.5. Protección y prevención de incendios

Los Centros de Proceso de Datos de la ACEDICOM disponen de sistemas automatizados para la detección y extinción de incendios.

### 5.1.6. Sistema de almacenamiento

Los soportes de información sensible se almacenan de forma segura en armarios ignífugos y cajas fuertes, según el tipo de soporte y la clasificación de la información en ellos contenida.

Estos armarios se encuentran en diversas dependencias para eliminar riesgos asociados a una única ubicación. El acceso a estos soportes está restringido a personal autorizado.

### 5.1.7. Eliminación de residuos

La eliminación de soportes magnéticos, ópticos e información en papel se realiza de forma segura siguiendo procedimientos establecidos para este fin, adoptando procesos de formateo, borrado permanente, de destrucción o triturado en función del tipo soporte a tratar.

### 5.1.8. Backup remoto

Diariamente se realizan copias de backup remotas, siendo almacenadas en dependencias próximas al Centro de Proceso de Datos de respaldo, donde las operaciones de la ACEDICOM continuarían en caso de incidente grave o caída del Centro de Proceso de Datos principal.

## 5.2. CONTROLES DE PROCEDIMIENTOS

Los sistemas de información y los servicios de la ACEDICOM se operan de forma segura, siguiendo procedimientos preestablecidos.

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se explican de forma resumida.

### 5.2.1. Papeles de confianza

Las personas que tengan que ocupar estos sitios son formalmente nominados por la alta dirección de EDICOM.

Las funciones fiables incluyen:

#### Operadores de Registro

Comprobarán la identidad del solicitante y creará la "End Entity" en las CA mediante un formulario web. La autenticación en ese formulario será mediante smartcard exclusivamente sobre los equipos autorizados a tal efecto.

Esta operación de creación de "End entity" se quedará como "pendiente" y deberá ser aprobada por otro Operador de Registro diferente al que ha creado la solicitud.

#### Administrador de sistemas

No tendrán acceso a las claves de la CA.

No tendrán acceso a los logs de la CA. Se evitará mediante propiedades del usuario del software de CA.

Se autenticarán via smartcard con el software de CA y no admitirá este software otro método alternativo de autenticación.

#### Administrador del HSM

Serán los encargados de generar las claves físicas de la CA en el HSM y tendrán acceso a dichas claves dentro del HSM. No tendrán acceso a las copias de dichas claves. También intervendrán en el proceso de activación de la CA y de recuperación de claves en el HSM ante contingencias.

### Operador de sistemas.

Las funciones serán de backup y de operación en general. Este rol no es incompatible con el de administrador de sistemas.

### Auditor del sistema

Autorizado a ver logs de CA y auditarlos. Los logs los verá a través de la interfaz web que ofrece la CA. Autenticación a través de smartcard.

Sólo tendrá acceso a los logs este Rol.

El Auditor debe encargarse de:

- . Comprobar el seguimiento de incidencias y eventos
- . Comprobar la protección de los sistemas (explotación de vulnerabilidades, logs de acceso, usuarios, etc.).
- . Comprobar alarmas y elementos de seguridad física

### Responsable de Seguridad

Responsable de la definición y verificación de todos los procedimientos de seguridad tanto física como informática.

Deberá encargarse de:

- . Constatar la existencia de toda la documentación requerida y enumerada
- . Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.

## 5.2.2. Número de personas requeridas por tarea

Se requieren al menos dos personas para la activación de claves de los dispositivos criptográficos hardware de generación y almacenamiento de claves. La modificación de los parámetros de configuración de la CA implica la autenticación por parte de dos personas autorizadas y con privilegios suficientes.

## 5.2.3. Identificación y autenticación para cada papel

Todos los usuarios autorizados de ACEDICOM se identifican mediante técnicas de acceso basadas en usuario y password que pueden ser sustituidos por tarjetas de identificación.

La autenticación se complementa con las correspondientes autorizaciones para acceder a determinados activos de información o sistemas de ACEDICOM.

Se utilizan en la medida de lo posible técnicas de secreto compartido para acceso a los recursos críticos.

## 5.3. CONTROLES DE SEGURIDAD DE PERSONAL

La ACEDICOM tiene en cuenta, en cuanto a los controles de personal, los siguientes aspectos:

- Se mantiene confidencialidad de la información, poniendo los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones y, fuera del ámbito laboral en aquello referente a la seguridad de las infraestructuras.
- Se es diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en este documento.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen soportes de información a niveles de seguridad inferiores.
- Se reporta al Responsable de Seguridad, lo más pronto posible, cualquier incidente que se considere que afecta a la seguridad de la infraestructura, o limitar la calidad del servicio.
- Se utilizan los activos de la infraestructura para las finalidades que les han sido encomendadas.
- Se exigen manuales o guías de usuario de los sistemas que utiliza, que permiten desarrollar su función correctamente.

- Se exige documentación escrita que marque sus funciones y medidas de seguridad a las que está sometido.
- El responsable de seguridad vela porque el punto anterior sea ejecutado, proveyendo a los responsables de área toda la información que fuera necesaria.
- No se instalan en ninguno de los sistemas de la infraestructura, software o hardware que no sea expresamente autorizado por escrito por el responsable de sistemas.
- No se accede voluntariamente, ni se elimina o altera información no destinada a su persona o perfil profesional.

### 5.3.1.Requerimientos de antecedentes, calificación, experiencia, y acreditación

La Autoridad de Certificación requiere que todo el personal que desarrolla tareas en sus instalaciones tenga la suficiente cualificación y experiencia en entornos similares.

Todo el personal debe cumplir los requerimientos de seguridad de la organización y deben poseer:

- Conocimientos y formación sobre entornos de certificación digital.
- Formación básica sobre seguridad en sistemas de información.
- Formación específica para su puesto.
- Título académico o experiencia en la industria equivalente
- Los roles de confianza deben estar libres de conflictos de intereses.

La calificación y la experiencia pueden suplirse mediante una formación y entrenamiento apropiados.

### 5.3.2.Procedimientos de comprobación de antecedentes

Mediante comprobación de Curriculum Vitae del personal. Se solicitará el certificado de penales a aquellas personas que ocuparán un rol de confianza o de gestión para verificar que no tiene antecedentes criminales graves para el caso de nuevas incorporaciones de personal.

### 5.3.3.Requerimientos de formación

El personal de la Autoridad de Certificación está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización.

Dicho plan de formación incluye los siguientes aspectos:

1. Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
2. Formación en seguridad de los sistemas de información.
3. Servicios proporcionados por la Autoridad de Certificación.
4. Conceptos básicos sobre PKI.
5. Declaración de Prácticas de Certificación y las Políticas de Certificación pertinentes.
6. Gestión de incidencias.

### 5.3.4.Requerimientos y frecuencia de actualización de la formación

Ante cambios tecnológicos del entorno, introducción de nuevas herramientas o modificación de procedimientos operativos, se llevará a cabo la formación adecuada para el personal afectado.

Ante cambios en la Declaración de Prácticas de Certificación, Políticas de Certificación u otros documentos relevantes, se llevarán a cabo sesiones formativas.

### 5.3.5.Frecuencia y secuencia de rotación de tareas

No se ha definido ningún plan de rotación en la asignación de sus tareas para el personal de la Autoridad de Certificación.

### 5.3.6.Sanciones por acciones no autorizadas

En el caso de comisión de una acción no autorizada con respecto a la operación de la Autoridad de Certificación se tomarán medidas disciplinarias. Se considerarán acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, la Autoridad de Certificación suspenderá el acceso de las personas involucradas a todos los sistemas de información de la Autoridad de Certificación de forma inmediata al conocimiento del hecho.

Adicionalmente, en función de la gravedad de las infracciones, se aplicarán acciones disciplinarias que contemplan la suspensión y el despido de la persona responsable de la acción dañosa.

### 5.3.7.Requerimientos de contratación de personal

Todo el personal de la Autoridad de Certificación está sujeto al deber de secreto mediante la firma del acuerdo de confidencialidad al incorporarse a su puesto. En dicho acuerdo, además, se obliga a desarrollar sus tareas de acuerdo con esta Declaración de Prácticas de Certificación, la Política de Seguridad de la Información de la ACEDICOM y los procedimientos aprobados de la ACEDICOM.

### 5.3.8.Documentación proporcionada al personal

La ACEDICOM suministra la documentación que estrictamente necesite su personal en cada momento, con el fin que sea suficientemente competente de acuerdo con lo establecido en la sección correspondiente de esta política.

### 5.3.9.Controles periódicos de cumplimiento

El control de que el personal posee los conocimientos necesarios se lleva a cabo al finalizar las sesiones formativas y discrecionalmente, por parte del profesorado encargado de impartir estos cursos.

Anualmente, el Responsable de Seguridad llevará a cabo una revisión de la adecuación de las autorizaciones otorgadas a los efectivos privilegios concedidos a los empleados.

### 5.3.10.Finalización de los contratos

En caso de finalización de la relación laboral del personal que desarrolla sus funciones en la ACEDICOM, el Responsable de Seguridad procederá a llevar a cabo las acciones o comprobaciones que se detallan en los puntos siguientes, bien directamente o dando instrucciones para ello al personal adecuado.

#### 5.3.10.1. Acceso a ubicaciones de la organización

Se deberá suprimir los privilegios de acceso del individuo a las instalaciones de la organización cuyo acceso sea restringido.

#### 5.3.10.2. Acceso a los Sistemas de Información

Se deberán suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización, con especial atención a los privilegios de administración y a los de acceso remoto.

#### 5.3.10.3. Acceso a la documentación

Supresión de acceso a toda información, a excepción de la considerada PÚBLICA.

#### 5.3.10.4. Información al resto de la organización

Se deberá informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios. De este modo se pretende minimizar la posibilidad de ataques de "ingeniería social" por parte del mismo.

## 5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

### 5.4.1. Tipos de eventos registrados

ACEDICOM registra todos los eventos relacionados con:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar claves y certificados.
- Intentos exitosos o fracasados de reactivaciones y renovaciones de certificados
- Intentos exitosos o fracasados de generar, firmar o emitir una CRL.
- Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de certificados.
- Intentos exitosos o fracasados de acceso a las instalaciones por parte de personal autorizado
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal

### 5.4.2. Frecuencia de procesado de logs

Los registros de auditoría se examinan al menos una vez a la semana en búsqueda de actividad sospechosa o no habitual. El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación que estos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría también tienen que estar documentadas.

### 5.4.3. Periodo de retención para los logs de auditoría

ACEDICOM retendrá todos los registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de cuatro (4) semanas para los pertenecientes a auditorías diarias, un (1) año para las mensuales y quince (15) años para los de auditorías anuales.

Destacar que los registros de auditorías anuales contienen todos los registros generados al menos durante el último año, sin excepción, ya que las copias de los registros se realizan siempre completas, nunca incrementales, y el procedimiento de consolidación asegura que en todo momento se tiene un año de registros en los sistemas.

### 5.4.4. Protección de los logs de auditoría

Los ficheros de registro, tanto manuales como electrónicos, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

### 5.4.5. Procedimientos de backup de los logs de auditoría

Se generan copias de soporte completas de registro de auditoría diariamente, protegidas criptográficamente para evitar su manipulación.

### 5.4.6. Sistema de recogida de información de auditoría (interno vs externo)

El sistema de recolección de auditorías de los sistemas de información de la ACEDICOM es una combinación de procesos automáticos y manuales ejecutados por los sistemas operativos, las aplicaciones de la ACEDICOM, y por el personal que las opera.

#### 5.4.7. Notificación al sujeto causa del evento

No estipulado.

#### 5.4.8. Análisis de vulnerabilidades

Se establece la realización de, al menos, un análisis mensual de vulnerabilidades y de seguridad perimetral. Es responsabilidad de los coordinadores de los equipos de análisis el informar a la ACEDICOM, a través del Responsable de Seguridad, de cualquier problema que impida la realización de las auditorías, o la entrega de la documentación resultante. Es responsabilidad de la ACEDICOM informar a los equipos auditores de la suspensión de los análisis.

Los análisis de seguridad implican el inicio de las tareas precisas para corregir las vulnerabilidades detectadas y la emisión de un contra-informe por parte de la ACEDICOM.

### 5.5. ARCHIVO DE INFORMACIONES Y REGISTROS

La ACEDICOM garantiza que toda la información relativa a los certificados se guarda durante quince (15) años desde el inicio del procedimiento de registro.

#### 5.5.1. Tipo de informaciones y eventos registrados

Las informaciones y eventos registrados son:

- Los registros de auditoría especificados en el punto 5.4 de esta Declaración de Prácticas de Certificación.
- Los soportes de backup de los servidores que componen la infraestructura de ACEDICOM.
- Documentación relativa al ciclo de vida de los certificados, entre la que se encuentra:
  - Contrato de certificación
  - Copia de la documentación de identificación aportada por el solicitante del certificado
  - Ubicación del Punto de Registro de Usuario -PRU- donde se emitió el certificado
  - Identidad del operador del PRU donde se emitió el certificado
  - Fecha de la última identificación cara a cara del suscriptor
- Acuerdos de confidencialidad
- Convenios suscritos por la ACEDICOM
- Autorizaciones de acceso a los Sistemas de Información (autorización de operador de Punto de Registro de Usuario, entre otras).

#### 5.5.2. Periodo de retención para el archivo.

Toda la información y documentación relativa al ciclo de vida de los certificados emitidos por ACEDICOM se conserva durante un periodo de quince (15) años.

#### 5.5.3. Protección del archivo.

El acceso al archivo se encuentra restringido a personal autorizado.

Asimismo los eventos relativos a los certificados emitidos por ACEDICOM se encuentra protegida criptográficamente para evitar las manipulaciones en su contenido.

#### 5.5.4. Procedimientos de backup del archivo.

Se realizan dos copias diarias de los ficheros que componen los archivos a retener.

Una copia se realiza en local y se almacena en una caja fuerte ignífuga dentro del Centro de Proceso de Datos principal de ACEDICOM.

La segunda copia de los datos se realiza de forma cifrada y remota y se almacena en el Centro de Proceso de Datos de continuidad o respaldo sito en un edificio distinto al del CDP principal de ACEDICOM.

#### 5.5.5.Requerimientos para el sellado de tiempo de los registros.

Los sistemas de ACEDICOM realizan el registro del instante de tiempo en los que se realizan. El tiempo de los sistemas proviene de una fuente fiable de hora. Todos los sistemas de ACEDICOM sincronizan su instante de tiempo con esta fuente. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se autocalibran por distintos caminos, utilizando como referencia entre otros la del Real Instituto y Observatorio de la Armada

#### 5.5.6.Sistema de recogida de información de auditoría (interno vs externo).

El sistema de recogida de información es interno a la entidad ACEDICOM.

#### 5.5.7.Procedimientos para obtener y verificar información archivada

Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

De forma automática se realizan comprobaciones de la integridad de los archivos electrónicos (backups), en tiempo de su generación y tras copiarlo al soporte de backup y se crea una incidencia en el caso de errores o comportamientos imprevistos.

### 5.6. CAMBIO DE CLAVE DE LA AC

Los procedimientos para proporcionar, en caso de cambio de claves de una AC, la nueva clave pública de AC a los titulares y terceros aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el sitio web <http://acedicom.edicomgroup.com>.

Los procedimientos para proporcionar una nueva clave pública a los usuarios de dicha AC corresponden al procedimiento de renovación recogido en este documento.

### 5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE

En el caso de una indisponibilidad de las instalaciones de la Autoridad de Certificación por un periodo superior a seis horas, se procederá a la activación del Plan de Recuperación de Desastres de la ACEDICOM.

El Plan de Recuperación de Desastres garantiza que los servicios identificados como críticos por su requerimiento de disponibilidad, estén disponibles en el CPD de continuidad en menos de 12 horas, tras la activación del Plan.

#### 5.7.1.Alteración de los recursos hardware, software y/o datos

Si los recursos hardware, software, y/o datos se alteran o son sospechosos de haber sido alterados se detendrá el funcionamiento de los servicios de la ACEDICOM hasta el restablecimiento de un entorno seguro con la incorporación de nuevos componentes de eficiencia acreditable. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no reproducción de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los suscriptores de los mismos y se procederá a su recertificación.

#### 5.7.2.La clave pública de una entidad se revoca

En el caso de la revocación del certificado de una entidad de ACEDICOM se generará y publicará la correspondiente CRL, se detendrá el funcionamiento de la entidad y se procederá a la

generación, certificación y puesta en marcha de una nueva entidad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso que la entidad afectada sea una CA el certificado revocado de la entidad permanecerá accesible en el repositorio de ACEDICOM con objeto de continuar permitiendo la verificación de los certificados emitidos durante su periodo de funcionamiento.

Las entidades componentes de ACEDICOM dependientes de la entidad renovada serán informadas del hecho y conminadas a solicitar su recertificación por la nueva instancia de la entidad.

### 5.7.3.La clave de una entidad se compromete

En el caso de compromiso de la clave de una entidad se procederá a su revocación inmediata según lo expuesto en el punto anterior y se informará del hecho al resto de entidades que componen ACEDICOM dependientes o no de la entidad afectada.

Los certificados firmados por entidades dependientes de la clave comprometida, en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, serán a su vez revocados, informados sus suscriptores y recertificados.

### 5.7.4.Instalación de seguridad después de un desastre natural u otro tipo de desastre

En caso de desastre natural que afecte a las instalaciones del Centro de Proceso de Datos principal de la ACEDICOM y, por tanto, a los servicios que desde éste se prestan, se activará el Plan de Recuperación de Desastres, garantizándose que los servicios identificados como críticos por su requerimiento de disponibilidad, estén disponibles en el CPD de continuidad en menos de 12 horas, tras la activación del Plan, y el resto de servicios imprescindibles dentro de plazos razonables y adecuados a su nivel de necesidad y criticidad.

## 5.8. CESE DE UNA CA

Las causas que pueden producir el cese de la actividad de la Autoridad de Certificación son:

- . Compromiso de la clave privada de la CA
- . Decisión política por parte de EDICOM

En caso de cese de su actividad como Prestador de Servicios de Certificación, ACEDICOM realizará, con una antelación mínima de dos meses, las siguientes acciones:

- . Informar a todos los suscriptores de sus certificados y extinguir la vigencia de los mismos revocándolos.
- . Informar a todas las terceras partes con las que tenga que haya firmado un convenio de certificación.
- . Comunicar al Ministerio competente en materia de Sociedad de la Información y firma electrónica el cese de su actividad y el destino que va a dar a los certificados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.
- . Remitir al Ministerio competente en materia de Sociedad de la Información y firma electrónica toda la información relativa a los certificados electrónicos revocados así como información de eventos y logs para que éste se haga cargo de su custodia durante el resto del periodo comprometido.
- . Revocar las autorizaciones para poder ejecutar el proceso de emisión de certificados a todo subcontratado que actúe en nombre o para la CA.
- . Destrucción de las claves privadas de la CA
- . La ACEDICOM no contempla la transferencia de la gestión de los certificados que todavía pudieran estar vigentes en el momento del cese de la CA, por lo que extinguirá la vigencia de todos los certificados en los términos establecidos en la Ley 59/2003.

## 6. CONTROLES DE SEGURIDAD TÉCNICA

La ACEDICOM utiliza sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

### 6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

#### 6.1.1. Generación del par de claves

Los pares de claves para los componentes internos de la PKI ACEDICOM, concretamente AC Raíz y ACs Subordinadas, se generan en módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

Los pares de claves para entidades finales se generan en función de lo estipulado en la Política de Certificación aplicable.

#### 6.1.2. Entrega de la clave privada a la entidad

En los casos en los que la generación de las claves no se realice mediante medios bajo control de la propia entidad final será la Política de Certificación correspondiente la que especifique el procedimiento a emplear para realizar la entrega de la clave privada a las entidades finales.

#### 6.1.3. Entrega de la clave pública al emisor del certificado

Las claves públicas generadas por medios bajo el control de las entidades finales se envían a ACEDICOM como parte de una solicitud de certificación en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

#### 6.1.4. Entrega de la clave pública de la CA a los usuarios

Las claves públicas de todas las CA pertenecientes a la jerarquía de confianza de ACEDICOM se pueden descargar del sitio web de ACEDICOM <http://acedicom.edicomgroup.com>

Se establecen medidas adicionales para confiar en el certificado auto firmado, como la comprobación de la huella digital del certificado.

#### 6.1.5. Tamaño de las claves

Las claves de la ACEDICOM Root y ACEDICOM Root son claves RSA de 4096 bits de longitud.

El tamaño de las claves para cada tipo de certificado emitido por ACEDICOM se establece en la Política de Certificación que le es de aplicación. En todo caso, su tamaño nunca será inferior a 1.024 bits.

#### 6.1.6. Parámetros de generación de la clave pública

Las claves de la ACEDICOM Root y ACEDICOM están creadas con el algoritmo RSA.

Los parámetros de generación de claves para cada tipo de certificado emitido por ACEDICOM vienen definidos por la Política de Certificación que le sea de aplicación.

En ambos casos las claves públicas están codificadas según RFC 3280 y PKCS#1.

#### 6.1.7. Comprobación de la calidad de los parámetros

Los procedimientos y medios de comprobación de la calidad de los parámetros de generación de claves para cada tipo de certificado emitido por ACEDICOM vienen definidos por la Política de Certificación que le sea de aplicación y en concreto de acuerdo con el informe especial del ETSI SR 001 276, que indica la calidad de los algoritmos de firma electrónica.

Los algoritmos y parámetros de firma utilizados por las Autoridades de Certificación ACEDICOM para la firma de certificados electrónicos y listas de certificados revocados son los siguientes:

**Signature algorithm Signature algorithm parameters**

Rsa MinModLen=1020

**Key generation algorithm**

rsagen1

**Padding method Cryptographic**

emsa-pkcs1-v1\_5

**Hash function**

sha1

### 6.1.8. Hardware/software de generación de claves

Los pares de claves de las Entidades de Certificación están generados utilizando hardware criptográfico que cumple los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por ACEDICOM viene definido por la Política de Certificación que le sea de aplicación.

### 6.1.9. Fines del uso de la clave

Los fines del uso de la clave para cada tipo de certificado emitido por ACEDICOM vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por ACEDICOM contienen las extensiones *KEY USAGE* y *EXTENDED KEY USAGE* definidas por el estándar X.509 v3 para la definición y limitación de tales fines.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por ACEDICOM.

## 6.2. PROTECCIÓN DE LA CLAVE PRIVADA

### 6.2.1. Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por AC Raíz y Acs *Subordinadas* de ACEDICOM cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

### 6.2.2. Control multipersona de la clave privada

La clave privada, tanto de la AC Raíz como de AC *Subordinada*, se encuentra bajo control multipersona. Ésta se activa mediante la inicialización del software de AC por medio de una combinación de operadores de la AC, administradores del HSM y usuarios de S.O.

Éste es el único método de activación de dicha clave privada.

Control multipersona: control por más de una persona, normalmente por un subconjunto 'k' de un total de 'n' personas. De esta forma, se garantiza que nadie tenga el control de forma individual de las actuaciones críticas a la vez que se facilita la disponibilidad de las personas necesarias.

### 6.2.3. Custodia de la clave privada

Se custodian claves privadas de firma de los suscriptores. Dichas claves y las claves privadas de las Autoridades de Certificación y Autoridades de Registro que componen ACEDICOM se encuentran alojadas en dispositivos de hardware criptográfico con certificación de seguridad FIPS 140-2 de nivel 3 cumpliendo los requisitos establecidos en un perfil de protección de dispositivo seguro de creación de firma y de firma electrónica de autoridad de certificación normalizado.

#### 6.2.4. Copia de seguridad de la clave privada

Las copias de backup de las claves privadas de componentes de ACEDICOM se almacenan cifradas en archivos seguros ignífugos. La clave privada de la AC sólo se puede exportar una vez en múltiples fragmentos que estarán en poder de diferentes personas.

#### 6.2.5. Archivo de la clave privada.

Las copias de backup de las claves privadas de algunos componentes de la ACEDICOM se custodiarán cifradas en archivos seguros ignífugos.

#### 6.2.6. Introducción de la clave privada en el módulo criptográfico.

Las claves privadas se crean en el módulo criptográfico en el momento de la creación de cada una de las entidades de ACEDICOM que hacen uso de dichos módulos.

#### 6.2.7. Método de activación de la clave privada.

La clave privada tanto de la ACEDICOM Root como de ACEDICOM se activa mediante la inicialización del software de CA y la activación del hardware criptográfico que contiene las claves.

#### 6.2.8. Método de desactivación de la clave privada

Un Administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación de ACEDICOM mediante la detención del software de CA.

#### 6.2.9. Método de destrucción de la clave privada

Las claves privadas son destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

No se contempla la destrucción de HSM, debido a su alto coste. En su lugar se procederá a las tareas de Inicialización del mismo. Durante el paso del estado "operacional" al de "inicialización" se produce el borrado seguro de las claves en él contenidas.

Se dispone de un procedimiento operativo de destrucción de las claves de la CA .

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

#### 6.2.10 Clasificación de los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por AC Raíz y Acs *Subordinadas* de ACEDICOM cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

### 6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.

#### 6.3.1. Archivo de la clave pública

La Infraestructura de Clave Pública de ACEDICOM, en cumplimiento de lo establecido por el artículo 20 f) de la LFE 59/2003 y en su vocación de permanencia mantendrá sus archivos por un periodo mínimo de quince años (15).

### 6.3.2.Periodo de uso para las claves públicas y privadas

El certificado de ACEDICOM Root tiene una validez de veinte (20) años. El de ACEDICOM de diez (10) años.

El periodo de validez de los certificados de entidades finales vendrá establecido por la Política de Certificación aplicable en cada caso, y en ningún caso superará los cuatro (4) años de validez máxima.

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

## 6.4. DATOS DE ACTIVACIÓN

### 6.4.1.Generación y activación de los datos de activación

Para la instauración de una Autoridad de Certificación del dominio de ACEDICOM se deben crear tarjetas criptográficas, que servirán para actividades de funcionamiento y recuperación. La AC opera con varios tipos de roles, cada uno con sus correspondientes tarjetas criptográficas donde se almacenan los datos de activación.

### 6.4.2.Protección de los datos de activación

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

### 6.4.3.Otros aspectos de los datos de activación

No estipulado.

## 6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

### 6.5.1 Requisitos técnicos específicos de seguridad informática

Se garantiza que el acceso a los sistemas está limitado a individuos debidamente autorizados. En particular:

- La ACEDICOM garantiza una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como de cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo la gestión de cuentas de usuario, auditoría y modificaciones o denegaciones de acceso oportunas.
- La ACEDICOM garantiza que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas de la Entidad, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema esta restringido y estrechamente controlado.
- El personal de la Entidad está identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal de la Entidad es responsable y tiene que poder justificar sus actividades, por ejemplo mediante un archivo de acontecimientos.
- Tiene que evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenaje (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.

- Los sistemas de seguridad y monitorización permiten una rápida detección, registro y actuación ante intentos de acceso irregulares o no autorizados a sus recursos (por ejemplo, mediante un sistema de detección de intrusiones, monitorización y alarma).
- El acceso a los depósitos públicos de la información de la ACEDICOM (por ejemplo, certificados o información de estado de revocación) cuenta con un control de accesos para modificaciones o borrado de datos.

### 6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de CA son fiables, de acuerdo con la especificación técnica CEN CWA 14167-1, evaluándose el grado de cumplimiento mediante un perfil de protección adecuado, de acuerdo con la norma ISO 15408 o equivalente.

## 6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.

### 6.6.1 Controles de desarrollo de sistemas

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizada en las aplicaciones de Autoridad (técnica) de certificación y de Autoridad (técnica) de Registro, para garantizar que los sistemas son seguros.

Se utilizan procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

### 6.6.2 Controles de gestión de seguridad

La ACEDICOM mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección correspondiente de este documento.

Los sistemas de la ACEDICOM se protegen contra virus y software no autorizado y malintencionado.

Se realiza un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenaje para los activos informativos.

## 6.7. CONTROLES DE SEGURIDAD DE LA RED

Se garantiza que el acceso a las diferentes redes de la ACEDICOM es limitado a individuos debidamente autorizados. En particular:

- Se implementan controles (como por ejemplo cortafuegos) para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la ACEDICOM.
- Los datos sensibles se protegen cuando se intercambian a través de redes no seguras (incluyendo los datos de registro del suscriptor).
- Se garantiza que los componentes locales de red (como direccionadores) se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

## 6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

ACEDICOM utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros.

ACEDICOM únicamente utiliza módulos criptográficos con certificación FIPS 140-2 o ITSEC E3 o superior.

## 7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

### 7.1. PERFIL DE CERTIFICADO

Los certificados emitidos por el sistema de la ACEDICOM serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la TS 101 862)

#### 7.1.1. Número de versión

ACEDICOM soporta y utiliza certificados X.509 versión 3 (X.509 v3) X.509 es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Clave Pública y los Certificados digitales.

#### 7.1.2. Extensiones del certificado

Las extensiones utilizadas en los certificados son:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *Subject Directory Attributes*. Calificada como no crítica.
- *CRLDistributionPoints*. Calificada como no crítica.
- *Authority Information Access*. Calificada como no crítica.
- *Qcstatements*. Calificada como no crítica.

ACEDICOM tiene definida una política de asignación de OID's dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de ACEDICOM comienzan con el prefijo 1.3.6.1.4.1.30051.3.1

ACEDICOM tiene definidas las siguientes extensiones propietarias:

OID	Concepto Descripción
1.3.6.1.4.1.30051.3.1.1	CIF de la organización representada

El perfil de cada certificado se detalla en cada una de las políticas correspondientes.

#### 7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA1withRSAEncryption (1.2.840.113549.1.1.5)

#### 7.1.4. Formatos de nombres

Los certificados emitidos por ACEDICOM contienen el *distinguished name* X.500 del emisor y el suscriptor del certificado en los campos *issuer name* y *subject name* respectivamente.

El campo *cn* del *subject name* se cumplimenta obligatoriamente en mayúsculas, prescindiendo de acentos y sustituyendo la letra "Ñ" por la "N" y la letra "Ç" por la "C". Esta característica se da únicamente en el atributo *CommonName*.

### 7.1.5. Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

### 7.1.6. Identificador de objeto (OID) de la Política de Certificación

El identificador de objeto definido por ACEDICOM para identificar la presente práctica de certificación es el siguiente: 1.3.6.1.4.1.30051.2.1.1.1

### 7.1.7. Uso de la extensión "Policy Constraints"

No estipulado

### 7.1.8. Sintaxis y semántica de los cualificadores de política

No estipulado

### 7.1.9. Tratamiento semántico para la extensión crítica "Certificate Policy"

La extensión "*Certificate Policy*" identifica la política que define las practicas que ACEDICOM asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

## 7.2. Perfil de CRL

### 7.2.1. Número de versión

El formato de las CRLs utilizadas en la presente política es el especificado en la versión 2 (X509 v2).

### 7.2.2. CRL y extensiones

La presente Declaración de Prácticas de Certificación soporta y utiliza CRLs conformes al estándar X.509.

## 7.3 LISTAS DE CERTIFICADOS REVOCADOS

### 7.3.1 Limite Temporal de los certificados en las CRLs

Los números de serie de los certificados revocados aparecerán en las CRL hasta que alcancen su fecha de expiración.

## 7.4.- PERFIL DE OCSP

### 7.4.1.- Perfil del certificado OCSP responder

Los certificados de OCSP responder serán emitidos por AC subordinada correspondiente del dominio de certificación de la ACEDICOM y serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- IETF RFC 2560 Online Certificate Status Protocol – **OCSP**

El periodo de validez de los mismos será no superior a 2 años. Tal y como contempla la RFC 2560, la AC emisora incluirá en el certificado de OCSP responder la extensión “*idpkix-ocsp-nocheck*” para indicar que los clientes OCSP deben confiar en el prestador de servicios de validación durante el periodo de vida del certificado asociado. No obstante, la AC no descarta en un futuro incluir en la extensión AIA de los certificados de OCSP responder información acerca de mecanismos adicionales para comprobar la validez de dichos certificados.

#### 7.4.2.- Número de versión

Los certificados de OCSP Responder utilizarán el estándar X.509 versión 3 (X.509 v3)

#### 7.4.3.- Formatos de nombres

Los certificados de OCSP Responder emitidos por una AC del dominio de ACEDICOM contendrán el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

Los nombres contenidos en los certificados están restringidos a ‘Distinguished Names’ X.500, que son únicos y no ambiguos.

El DN para los certificados estará compuesto de los siguientes elementos:

CN, OU, O, C

El atributo “C” (countryName) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString, el resto de atributos se codificarán en UTF8:

CN=OCSPSignerCertificate

CN=ACEDICOM XX

OU=PKI

O=EDICOM

L=Ronda de Auguste y Louis Lumiere 12 Paterna

ST=Valencia,

C=ES

serialNumber=B96490867

postalCode=46980

emailAddress=acedicom@edicomgroup.com

donde XX es el código cada una de las CA subordinadas (01,02, etc.)

#### 7.4.4.- Identificador de objeto (OID) de la Política de Certificación

No estipulado

#### 7.4.5.- Extensiones y campos del certificado

El perfil del certificado del OCSP responder que emite la PKI ACEDICOM es:

CAMPO	CONTENIDO	CRÍTICA para extensiones
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Número único asignado por la CA	
3. Signature Algorithm	SHA1withRSAEncryption	
4. Issuer Distinguished Name	CN=ACEDICOM XX OU=PKI O=EDICOM L=Ronda de Auguste y Louis Lumiere 12 Paterna ST=Valencia, C=ES serialNumber=B96490867 postalCode=46980	

	emailAddress=acedicom@edicomgroup.com	
5. Validez	2 años	
6. Subject	CN=OCSPSignerCertificate CN=ACEDICOM XX OU=PKI O=EDICOM L=Ronda de Auguste y Louis Lumiere 12 Paterna ST=Valencia, C=ES serialNumber=B96490867 postalCode=46980 emailAddress=acedicom@edicomgroup.com	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048 bits	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora.	NO
3. KeyUsage	DigitalSignature	SI
4. extKeyUsage	OCSPSigning	
14. OCSPNoCheck	Valor NULL como contempla la norma	NO

#### 7.4.6.- Formato peticiones OCSP

Se soporta la extensión Nonce (id-pkix-ocsp-nonce) tal y como contempla la norma para evitar "replay attacks".

#### 7.4.7.- Formato de las respuestas

El OCSP responder del servicio de validación es capaz, al menos, de generar respuestas de tipo id-pkix-ocsp-basic.

Respecto al estado de los certificados deberá responder como:

- "Revoked", para aquellos certificados emitidos por las AC del dominio de certificación de la ACEDICOM y que consten en las CRLs
- "Good", para aquellos certificados emitidos por las AC del dominio de certificación de la ACEDICOM y que no consten en las CRLs. El estado "good" es simplemente una respuesta "positiva" a la petición OCSP, indica que el certificado no está revocado pero no implica necesariamente que el certificado fue emitido alguna vez o que se encuentra dentro del periodo de validez.
- "unknown" si la petición corresponde a una AC emisora desconocida

Respecto a la semántica de los campos thisUpdate, nextupdate y producedAt.

- "producedAt" deberá contener el instante de tiempo en el que el OCSP responder genera y firma la respuesta
- "thisUpdate", debe indicar el momento en el que se sabe que el estado indicado en la respuesta es correcto. En el caso de certificados revocados deberá contener el campo "thisUpdate" de la CRL que se haya utilizado. En el resto de casos se utilizará la fecha local.
- "nextUpdate", debe indicar el instante de tiempo en el que se dispondrá de nueva información de revocación. En el caso de certificados revocados deberá contener el campo "nextUpdate" de la CRL que se ha utilizado, salvo cuando la fecha de "nextUpdate" sea anterior a la fecha local. En el resto de casos no se establecerá el campo nextUpdate, lo que es equivalente según rfc2560 a indicar que se puede disponer de nueva información de revocación en cualquier momento, con lo que es responsabilidad del cliente volver a consultar cuando lo estime oportuno

## 8. AUDITORÍA DE CONFORMIDAD

### 8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD

Se llevará a cabo una auditoría sobre ACEDICOM, al menos una vez al año, para garantizar la adecuación de su funcionamiento y operativa con las disposiciones incluidas en esta CPS.

Se llevarán a cabo otras auditorías técnicas y de seguridad, entre las que se incluye una auditoría de cumplimiento de la legislación de protección de datos de carácter personal.

### 8.2. IDENTIFICACION/CUALIFICACIÓN DEL AUDITOR

El auditor será seleccionado en el momento de la realización de cada auditoría.

Si la ACEDICOM dispone de un departamento de auditoría interna, éste puede encargarse de realizar la auditoría de conformidad.

En el caso de no poseer este departamento, la ACEDICOM puede acudir a un auditor independiente externo, el cual tiene que demostrar experiencia en seguridad informática, en seguridad de Sistemas de Información y/o en auditorías de conformidad de Autoridades de Certificación y los elementos relacionados.

### 8.3. RELACION ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Al margen de la función de auditoría, el auditor y la parte auditada (ACEDICOM) no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses.

En cumplimiento de lo establecido en la normativa vigente en nuestro ordenamiento sobre protección de datos de carácter personal, y habida cuenta de que para el cumplimiento, por parte del auditor, de los servicios regulados en el contrato será preciso acceder a los datos de carácter personal de los ficheros titularidad de la ACEDICOM, el auditor tendrá la consideración de Encargado de Tratamiento, en virtud de lo previsto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de Diciembre.

### 8.4. TOPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD

La auditoría determinará la conformidad de los servicios de ACEDICOM con esta CPS y las CP's aplicables. También determinará los riesgos del no cumplimiento de la adecuación con la operativa definida por esos documentos.

Los aspectos cubiertos por una auditoría incluirá, pero no estará limitada a:

- Política de seguridad.
- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la CA
- CPS y CP's vigentes

### 8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.

Una vez recibido el informe de la auditoría de cumplimiento llevada a término, la ACEDICOM discute, con la entidad que ha ejecutado la auditoría las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que soluciona dichas deficiencias.

Si ACEDICOM auditada es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema tiene que realizarse una de las siguientes acciones:

- Revocar la clave de la ACEDICOM, de la forma como se describe en las secciones correspondientes de esta política.

- Finalizar la prestación del servicio de la ACEDICOM, de la forma como se describe en la sección correspondiente de esta política.

## 8.6. COMUNICACIÓN DE RESULTADOS

El auditor comunicará los resultados de la auditoría al Director Técnico de EDICOM, en tanto que responsable máximo de la ACEDICOM, al Responsable de Seguridad de ACEDICOM, así como a los responsables de las distintas áreas en las que se detecten no conformidades.

## 9. REQUISITOS COMERCIALES Y LEGALES

### 9.1. TARIFAS

#### 9.1.1. Tarifas de emisión de certificado o renovación

Las tarifas de emisión y revocación de cada certificado se especifican en el repositorio público de la ACEDICOM: <http://acedicom.edicomgroup.com>

#### 9.1.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos, dada su naturaleza pública, es libre y gratuito y por tanto no es de aplicación ninguna tarifa sobre los mismos.

#### 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 basado en CRLs es libre y gratuito y por tanto no se le aplica ninguna tarificación. El acceso al servicio OCSP responder, puede tarifarse a criterio de ACEDICOM. En su caso, las tarifas de este servicio se publicarán en el repositorio público de la ACEDICOM: <http://acedicom.edicomgroup.com>

#### 9.1.4. Tarifas de otros servicios como información de políticas

No se aplicará ninguna tarifa por el servicio de información sobre esta CPS ni las políticas de certificación administradas por ACEDICOM ni por ningún otro servicio adicional distinto a los "Servicios de firma electrónica" del que se tenga conocimiento en el momento de la redacción del presente documento.

Esta disposición podrá ser modificada por la Política de Certificación aplicable en cada caso.

#### 9.1.5. Política de reintegros

Sin estipulación adicional.

### 9.2. CAPACIDAD FINANCIERA

#### 9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACEDICOM.

La ACEDICOM, en su actividad como prestador de servicios de Certificación dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, no obstante su responsabilidad en el ejercicio de la actividad de PSC tal como se define en la legislación española vigente en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre (de firma electrónica), queda garantizada mediante un Seguro de Responsabilidad Civil Profesional con una cobertura de Tres millones de Euros (3.000.000 €).

#### 9.2.2. Relaciones fiduciarias

ACEDICOM no se desempeña como agente fiduciario ni representante en forma alguna de suscriptores ni de terceros que confían en los certificados emitidos por la ACEDICOM.

#### 9.2.3. Procesos administrativos

ACEDICOM garantiza la realización de auditorías de los procesos y procedimientos establecidos de manera regular. Estas auditorías se llevarán a cabo tanto de manera interna como externa.

## 9.3. POLÍTICA DE CONFIDENCIALIDAD

### 9.3.1. Información confidencial.

Se declara expresamente como información confidencial, que no podrá ser divulgada a terceros, excepto en aquellos supuestos previstos legalmente:

- Las claves privadas de las entidades que componen ACEDICOM.
- Las claves privadas de suscriptores de las que ACEDICOM mantenga en custodia.
- Toda información relativa a las operaciones que lleve a cabo ACEDICOM.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a ACEDICOM durante el proceso de registro de los suscriptores de certificados, con la salvedad de lo especificado por la Política de Certificación aplicable y el contrato de certificación.
- La información de negocio suministrada por sus proveedores y otras personas con las que la ACEDICOM tiene el deber de guardar secreto establecida legal o convencionalmente.
- Planes de continuidad de negocio y de emergencia.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Toda la información clasificada como "CONFIDENCIAL" o "ESTRICTAMENTE CONFIDENCIAL"

### 9.3.2. Información no confidencial

ACEDICOM considera información de acceso público:

- La contenida en la Declaración de Prácticas de Certificación aprobada por la ACEDICOM.
- La contenida en las diferentes Políticas de Certificación aprobadas por la ACEDICOM.
- Los certificados emitidos así como las informaciones contenidas en éstos.
- La lista de certificados revocados (CRL)
- Toda aquella información que sea calificada como "PÚBLICA".

La CPS y las CP's de la ACEDICOM no incluirán información calificada como confidencial en el punto 9.3.1 del presente documento.

Se permite el acceso a la información no considerada confidencial, sin perjuicio de que se establezcan por la ACEDICOM los controles de seguridad pertinentes con el fin de proteger la autenticidad e integridad de los documentos que albergan la información de acceso público e impedir así que personas no autorizadas puedan añadir, modificar o suprimir contenidos.

### 9.3.3. Divulgación de información de revocación /suspensión de certificados

La información relativa a la revocación o suspensión de certificados se proporciona vía CRL.

## 9.4. PROTECCIÓN DE DATOS PERSONALES

La ACEDICOM dispone de una Política de Privacidad, publicada en la web de ACEDICOM, mediante la que se da cumplimiento a las disposiciones establecidas en la legislación de protección de datos de carácter personal vigente y en la que se informa sobre la política de protección de datos de carácter personal de la ACEDICOM.

### 9.4.1. Plan de Protección de Datos Personales.

La ACEDICOM desarrolla una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La Entidad de Certificación no divulga ni cede datos personales, excepto en los casos previstos, así como en la sección 5.8, en caso de finalización de la Entidad de Certificación.

La ACEDICOM dispone de los procedimientos en este documento, que aplica en la prestación de sus servicios, en el que, en cumplimiento de los requisitos establecidos por las políticas de

certificados que gestiona, y de acuerdo con el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, se detallan los requisitos y obligaciones en relación con la obtención y gestión de los datos personales que obtenga, cumpliendo a este efecto, las disposiciones de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, y del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

En concreto, las siguientes secciones del Reglamento de Medidas de Seguridad se cumplen con los controles de las siguientes secciones de este documento:

- a. Ámbito de aplicación del documento de seguridad con especificación detallada de los recursos protegidos – sección 9.4.
- b. Medidas, normas, procedimientos, reglas y estándares que garanticen el nivel de seguridad exigido por el Reglamento – sección 9.4, y, en general, todos los controles técnicos de las secciones 5 y 6.
- c. Funciones y obligaciones del personal – sección 5.3.
- d. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los traten – sección 9.4.2 y sección 1.3.1 respectivamente.
- e. Procedimiento de notificación, gestión y respuesta ante las incidencias – sección 9.4.4.
- f. Procedimientos de backup y recuperación de datos – sección 5.5.

#### 9.4.2. Información considerada privada.

De conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

Tanto la información personal que no haya de ser incluida en los certificados como el mecanismo de comprobación del estado de los certificados, se consideran información personal de carácter privado.

En cualquier caso, los siguientes datos son considerados como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados.
- Claves privadas generadas y/o almacenadas por la ACEDICOM.
- Toda otra información identificada como “Información privada”

Asimismo, los datos captados por el Prestador de Servicios de Certificación tienen la consideración legal de datos de nivel básico.

De conformidad con la Ley Orgánica 15/99 la información confidencial está protegida frente a su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

En ningún caso la ACEDICOM incluye en los certificados electrónicos que expide, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

#### 9.4.3. Información no considerada privada.

Esta información hace referencia a la información personal que se incluye en los certificados y en el referido mecanismo de comprobación del estado de los certificados, de acuerdo con la sección 3.1 de este documento.

Dicha información, proporcionada en la solicitud de certificados en los términos que se prevén en el artículo 17.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, es incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados.

La información no tiene carácter privado, por imperativo legal (“datos públicos”), pero solo se publica en el depósito si lo consiente el suscriptor.

En todo caso, es considerada no confidencial la siguiente información:

- a. Los certificados emitidos o en trámite de emisión

- b. La sujeción del suscriptor a un certificado emitido por la ACEDICOM.
- c. El nombre y los apellidos del suscriptor del certificado, así como cualesquiera otras circunstancias o datos personales del titular, en el supuesto que sean significativas en función de la finalidad del certificado, de acuerdo con este documento.
- d. La dirección electrónica del suscriptor del certificado.
- e. Los usos y límites económicos reseñados en el certificado.
- f. El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- g. El número de serie del certificado.
- h. Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- i. Las listas de revocación de certificados (LRCs), así como el resto de informaciones de estado de revocación.
- j. La información contenida en el Depósito de la ACEDICOM.

#### 9.4.4.Responsabilidades.

La ACEDICOM garantiza el cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley 59/2003, de 19 de diciembre, y en virtud de esto, y de acuerdo con el artículo 22 de dicha Ley, responderá por los daños y perjuicios que cause en el ejercicio de la actividad por el incumplimiento de las prescripciones contenidas en el artículo 17 de la Ley 59/2003, relativas a la protección de datos personales.

La ACEDICOM incluye en este documento su procedimiento de notificación, gestión y respuesta ante las incidencias relacionadas con los datos personales.

Este procedimiento contiene un registro en el que se hace constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, la persona a quien se comunica la notificación y los efectos que se derivan.

La ACEDICOM implanta medidas de identificación y autenticación, así como el necesario control de acceso del personal a los datos personales, controles que detallan las secciones 4 y 5 de este documento.

Los procedimientos de gestión de los soportes de datos personales y de los backups definidos en las secciones 5.5 de este documento cumplen los requisitos de los artículos 13 y 14 del Real Decreto 994/99.

#### 9.4.5.Prestación del consentimiento en el uso de los datos personales.

Para la prestación del servicio, la ACEDICOM habrá de obtener el consentimiento de los titulares de los datos necesarios para prestación los servicios de certificación. Se entenderá obtenido el consentimiento con la firma del contrato de certificación por parte del usuario.

#### 9.4.6.Comunicación de la información a autoridades administrativas y/o judiciales.

La ACEDICOM sólo podrá comunicar informaciones calificadas como confidencial o que contengan datos de carácter personal en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

En concreto, la ACEDICOM está obligada a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tengan atribuidas, y en el resto de supuestos previstos en el artículo 11.2 de la LOPD donde así se requiera.

#### 9.4.7.Otros supuestos de divulgación de la información.

La ACEDICOM incluye, en la política de privacidad prevista al inicio de la sección 9.4, prescripciones para permitir la divulgación de la información del poseedor de claves, directamente a los mismos o a terceros.

## 9.5. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual incluyendo los referidos a certificados y CRL's emitidos por la ACEDICOM, OIDs, la presente CPS, las Políticas de Certificación que le son de aplicación, así como cualquier otro documento, electrónico o de cualquier otro tipo, propiedad de ACEDICOM, pertenecen a la ACEDICOM.

Las claves privadas y las claves públicas son propiedad del usuario, independientemente del medio físico que se emplee para su almacenamiento.

El suscriptor conserva cualquier derecho que pudiere ostentar sobre la marca producto o nombre comercial contenido en el certificado.

## 9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL

### 9.6.1. Obligaciones de la Entidad de Certificación

#### 9.6.1.1 Obligaciones y otros compromisos

La ACEDICOM se obliga a cumplir lo siguiente:

- a. La ACEDICOM garantiza bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en este documento.
- b. La ACEDICOM es la única entidad responsable del cumplimiento de los procedimientos descritos en este documento, incluido cuando una parte o la totalidad de las operaciones son subcontratadas externamente.
- c. La ACEDICOM presta sus servicios de certificación de acuerdo con este documento, en el que se detallan al menos los contenidos previstos en el artículo 19 de la Ley 59/2003.
- d. Antes de la emisión y entrega del certificado al suscriptor, la ACEDICOM lo informa de los aspectos previstos en el artículo 18.b) de la Ley 59/2003, y de los siguientes aspectos:
  - a) Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad, en su caso, de utilización de dispositivo seguro de creación de firma
  - b) Forma en que se garantiza la responsabilidad patrimonial de la ACEDICOM
  - c) Si la ACEDICOM es declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema. En concreto, la certificación del prestador de servicios de certificación y la certificación de los productos de firma electrónica utilizados.
- e. Este requisito se cumple mediante la puesta a su disposición del documento de Declaración de Prácticas de Certificación de la ACEDICOM así como del documento de la Política de Certificación aplicable al tipo de certificado expedido.
- f. La ACEDICOM obliga a los suscriptores y a los verificadores mediante instrumentos jurídicos apropiados en cada situación.
- g. Estos instrumentos jurídicos pueden ser transmitidos electrónicamente, están en lenguaje escrito y comprensible, y tienen los siguientes contenidos mínimos:
  - a) Prescripciones para dar cumplimiento a lo establecido en la presente política de certificación.
  - b) Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de uso del dispositivo seguro de creación de firma.
  - c) Manifestación que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
  - d) Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
  - e) Consentimiento para el almacenaje de la información utilizada para el registro del suscriptor, para la provisión del dispositivo seguro de creación de firma y para la cesión de dicha información a terceros, en caso de finalización de operaciones de la ACEDICOM sin revocación de certificados válidos.

- f) Límites de uso del certificado, incluyendo las establecidas en la sección 4.5 de este documento.
- g) Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las que se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como verificador.
- h) Limitaciones de responsabilidad aplicables, incluyendo los usos por los que la ACEDICOM acepta o excluye su responsabilidad.
- i) Procedimientos aplicables de resolución de disputas.
- j) Ley aplicable y jurisdicción competente.
- k) La ACEDICOM tiene que identificar al suscriptor del certificado, de acuerdo con los artículos 12 y 13 de la Ley 59/2003 y el presente documento y, en concreto:
  - a) La ACEDICOM comprueba por si misma o por medio de una Entidad de Registro, la identidad y cualquier otras circunstancias personales de los solicitantes de los certificados, de acuerdo con lo establecido en el artículo 13 de la Ley 59/2003.
  - b) La ACEDICOM cumple el resto de obligaciones contenidas en el artículo 12 de la Ley 59/2003.

La ACEDICOM asume otras obligaciones incorporadas directamente en el certificado o incorporadas por referencia.

Nota: La incorporación por referencia se consigue incluyendo en el certificado un identificador de objeto u otra forma de enlace a un documento, que se considera incluido de forma íntegra en este documento.

Adicionalmente a lo establecido en la sección correspondiente, el instrumento jurídico que vincula la ACEDICOM y el suscriptor está en lenguaje escrito y comprensible, y tiene los siguientes contenidos mínimos:

- a. Indicación de que los certificados se expiden al público y de la necesidad, en su caso, de uso de dispositivo seguro de creación de firma, como se indica en la sección 6.2.8 de este documento.
- b. Certificación de servicios de la ACEDICOM.
- c. Forma en que se garantiza la responsabilidad patrimonial de la ACEDICOM.

### 9.6.1.2 Garantías ofrecidas a suscriptores y verificadores

La ACEDICOM, como mínimo, garantiza al suscriptor:

- a. El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con la Ley 59/2003, de 19 de diciembre.
- b. Que no haya errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la ACEDICOM y, en su caso, por la Entidad de Registro.
- c. Que no haya errores de hecho en las informaciones contenidas en los certificados, debidos a falta de diligencia en la gestión de la solicitud de certificado o a la creación de éste.
- d. Que los certificados cumplan todos los requisitos materiales establecidos en la DPC.
- e. La responsabilidad de la ACEDICOM, con los límites que se establezcan.
- f. Que los servicios de revocación y el uso del Depósito cumplen todos los requisitos materiales establecidos en la DPC.

La ACEDICOM, como mínimo, garantiza al verificador:

- a. Que, en el caso que genere las claves privadas del suscriptor o, en su caso, el poseedor de claves, se mantiene su confidencialidad durante el proceso.
- b. El cumplimiento de sus obligaciones legales como prestador de servicios de certificación, de acuerdo con la Ley 59/2003, de 19 de diciembre.
- c. Que la información contenido o incorporada por referencia al certificado es correcta.
- d. En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en éste y que el certificado ha sido aceptado, de acuerdo con la sección correspondiente del presente documento.

- e. Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en este documento.
- f. La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, la Entidad de Certificación garantiza al suscriptor y al verificador:

- a. Que el certificado contiene las informaciones que tiene que contener un certificado reconocido, de acuerdo con el artículo 11.2 de la Ley 59/2003, de 19 de diciembre.

### 9.6.2.Obligaciones de la Autoridad de Registro

- Las personas que operan en las RAs integradas en la jerarquía de ACEDICOM –operadores de Punto de Registro de Usuario– están obligadas a:
- Realizar sus operaciones en conformidad con esta CPS.
- Realizar sus operaciones de acuerdo con la Política de Certificación que sea de aplicación para el tipo de certificado solicitado en cada ocasión.
- Comprobar exhaustivamente la identidad de las personas a las que se les concede el certificado digital por ellos tramitado, para lo que requerirán la presencia física del solicitante y la exhibición de un documento nacional de identidad válido, original y en vigor. En caso de usuarios extranjeros deberán mostrar la Tarjeta de Residencia / NIE (o documento análogo y oficial de identidad)
- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de la ACEDICOM, la CPS y las CP vigentes y anteriores, la legislación aplicable, las certificaciones obtenidas y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de la actividad.
- Validar y enviar de forma segura a la CA a la que está subordinada la RA una solicitud de certificación debidamente cumplimentada con la información aportada por el suscriptor, y recibir los datos asociados a los certificados emitidos de acuerdo con esa solicitud.
- Almacenar de forma segura y hasta el momento de su remisión a la Autoridad de Certificación, tanto la documentación aportada por el suscriptor como la generada por la propia RA, durante el proceso de registro o revocación
- Formalizar el Contrato de Certificación con el suscriptor según lo establecido por la Política de Certificación aplicable.
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada.
- Autenticar las solicitudes de usuarios finales para la renovación o revocación de sus certificados, generar solicitudes de renovación o revocación firmadas digitalmente y enviarlas a su CA superior.
- En el caso de la aprobación de una solicitud de certificación notificar al suscriptor la emisión de sus certificados y la forma de obtenerlo.
- En el caso del rechazo de una solicitud de certificación, notificar al solicitante dicho rechazo y el motivo del mismo
- Mantener bajo su estricto control las herramientas de tramitación de certificados digitales y notificar a la Autoridad de Certificación EDICOM cualquier mal funcionamiento u otra eventualidad que pudiera salirse del comportamiento normal esperado.

- Remitir copia firmada del contrato de certificación y de las solicitudes de revocación a la Autoridad de Certificación EDICOM.
- Recibir y tramitar las solicitudes de revocación presenciales que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable basada en el DNI del demandante, o en el NIE en el caso de extranjeros.
- Colaborar en cuantos aspectos de la operación, auditoría o control del Punto de Registro de Usuario se le soliciten por parte de la Autoridad de Certificación.
- A la más general y amplia obligación de confidencialidad, durante y con posterioridad a la prestación del servicio como Autoridad de Registro, respecto de la información recibida por la ACEDICOM y respecto de la información y documentación en que se haya concretado el servicio. En el mismo sentido, no transmitir a terceros dicha información, bajo ningún concepto, sin autorización expresa, escrita y con carácter previo de la ACEDICOM, en cuyo caso trasladará a dichos terceros idéntica obligación de confidencialidad.

### 9.6.3.Obligaciones de los suscriptores

#### 9.6.3.1 Obligaciones y otros compromisos

La ACEDICOM obliga al suscriptor a:

- a. Facilitar a la ACEDICOM información completa y adecuada, en especial por lo que respecta al procedimiento de registro.
- b. Manifiestar su consentimiento previo a la emisión de un certificado.
- c. Cumplir las obligaciones que se establecen para el suscriptor en este documento y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- d. Utilizar el certificado de acuerdo con lo establecido en la sección correspondiente.
- e. Notificar a la ACEDICOM, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo seguro de creación de firma, si aplica.
- f. Notificar a la ACEDICOM y cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  - a) La pérdida, el robo o el compromiso potencial de su clave privada.
  - b) La pérdida de control sobre su clave privada, a causa del compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo seguro de creación de firma) o por cualquier otra causa.
  - c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- g. Dejar de utilizar la clave privada transcurrido el periodo indicado en la sección correspondiente.
- h. No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de la Jerarquía de la ACEDICOM, sin permiso previo por escrito.
- i. No comprometer intencionadamente la seguridad de la Jerarquía de ACEDICOM
- j. Utilizar el par de claves exclusivamente para firmas electrónicas y conforme a cualquiera otras limitaciones que le sean notificadas.
- k. Reconocer que estas firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre.
- l. Ser especialmente diligente en la custodia de su clave privada y de su dispositivo seguro de creación de firma (si aplica), con el fin de evitar usos no autorizados.
- m. En los casos en los que el suscriptor genera sus propias claves, se obliga a:
  1. Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica reconocida.
  2. Crear las claves dentro del dispositivo seguro de creación de firma.
  3. Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.

- n. Notificar a la EC, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo seguro de creación de firma.

### 9.6.3.2 Garantías ofrecidas por el suscriptor

La ACEDICOM obliga al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar:

- a. Que todas las manifestaciones realizadas en la solicitud son correctas.
- b. Que todas las informaciones suministradas por el suscriptor que se encuentre contenidas en el certificado son correctas.
- c. Que el certificado se utiliza exclusivamente para usos legales y autorizados, de acuerdo con la DPC de ACEDICOM.
- d. Que cada firma digital creada con la clave privada correspondiente a la clave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.
- e. Que el suscriptor es una entidad final y no una Entidad de Certificación, y no utiliza la clave privada correspondiente a la clave pública lista en el certificado para firmar ningún certificado (o cualquier otro formato de clave pública certificada), ni LRC.
- f. Que ninguna persona no autorizada ha tenido nunca acceso a la clave privada del suscriptor.

### 9.6.3.3 Protección de la clave privada

La ACEDICOM obliga al suscriptor, mediante el correspondiente instrumento jurídico, a garantizar que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

### 9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACEDICOM

- Es obligación de las partes que confíen en los certificados emitidos por ACEDICOM:
- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificado y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digitales
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

### 9.6.5. Obligaciones del repositorio

- Mantener accesible para las entidades finales el conjunto de certificados emitidos por ACEDICOM
- Mantener accesible para las entidades finales la información de los certificados que han sido revocados, en formato CRL.

## 9.7. RENUNCIAS DE GARANTÍAS

La ACEDICOM puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, especialmente aquellas garantías de adaptación para un propósito particular o garantía de uso mercantil del certificado.

## 9.8. LIMITACIONES DE RESPONSABILIDAD

### 9.8.1. Garantías y limitaciones de garantías

La ACEDICOM limita su responsabilidad restringiendo el servicio a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y depósitos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrado por la Entidad de Certificación. La ACEDICOM puede limitar su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede utilizarse el certificado.

### 9.8.2. Deslinde de responsabilidades

Las Entidades de Registro de ACEDICOM no asumen ninguna responsabilidad en caso de pérdida o perjuicio:

- De los servicios que prestan, en caso de guerra, desastres naturales o cualquier otro caso de fuerza mayor.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y esta CPS.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por ACEDICOM.
- Ocasionados al firmante o terceros de buena fe si el destinatario de los documentos firmados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la CRL, o cuando no verifique la firma electrónica

### 9.8.3. Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente CPS, ACEDICOM no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asumen ninguna otra responsabilidad ante suscriptores o partes confiantes.

## 9.9. PLAZO Y FINALIZACIÓN.

### 9.9.1. Plazo.

La ACEDICOM establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina el período de vigencia de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

### 9.9.2. Finalización.

La ACEDICOM establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

Una finalizada la actividad de CA se procederá a realizar los pasos indicados en el apartado 5.8.

### 9.9.3. Supervivencia.

La ACEDICOM establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de la que ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

A este efecto, la ACEDICOM vela porque, al menos los requisitos contenidos en las secciones Obligaciones, Responsabilidad civil, Auditoría de conformidad y Confidencialidad, continúen vigentes después de la finalización de la política de certificación y de los instrumentos jurídicos que vinculen la ACEDICOM con suscriptores y verificadores.

#### 9.10. NOTIFICACIONES.

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas descritas en esta CPS se realizará mediante documento o mensaje electrónico firmado digitalmente de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 1.5 *Datos de contacto*. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

Una finalizada la actividad de CA se procederá a realizar los pasos indicados en el apartado 5.8.

#### 9.11. MODIFICACIONES.

La ACEDICOM puede modificar unilateralmente este documento, sujetándose al siguiente procedimiento:

- La modificación tiene que estar justificada desde el punto de vista técnico y legal.
- La modificación propuesta por la ACEDICOM no puede vulnerar las disposiciones contenidas en las políticas de certificación establecidas por ACEDICOM.
- Se establece un control de modificaciones, para garantizar, en todo caso, que las especificaciones resultantes cumplan los requisitos que se intentan cumplir y que dieron pie al cambio.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones.

##### 9.11.1. Procedimientos de especificación de cambios

La entidad con atribuciones para realizar y aprobar cambios sobre la CPS y las CP's de la ACEDICOM es la Dirección Técnica de EDICOM, cuyos datos de contacto se encuentran en el apartado 1.5.1. de esta CPS.

En aquellos supuestos en los que se considere por la Dirección Técnica de EDICOM que la modificación de la CPS no reduce materialmente la confianza que una Política de Certificación o su implementación proporcionan, ni altera la aceptabilidad de los certificados que soporta la política para los propósitos para los que se han usado, se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los suscriptores de los certificados correspondientes a la CP o CPS modificada.

En el supuesto de que la Dirección Técnica de EDICOM juzgue que los cambios a la especificación vigente afecten a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del de Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los suscriptores de los certificados correspondientes a la CP o CPS modificada mediante el envío de una notificación a la dirección de correo electrónico que el usuario ha facilitado en la emisión del certificado, con una antelación de al menos 30 días a su publicación.

El usuario puede aceptar las modificaciones o rechazarlas:

- En caso de rechazarlas, su certificado, emitido bajo las instrucciones de la anterior CPS será válido para los propósitos en ella incluidos, pero no para los propósitos específicos que se incluyen en la nueva CPS o CP modificada. Si transcurridos 15 días desde la notificación al usuario no se tuviera respuesta del mismo, se considerará que el usuario no ha aceptado la modificación, aunque puede aceptarla en cualquier momento posterior.
- En caso de aceptarlas, tendrá lugar un procedimiento de recertificación en el cual el nuevo certificado solamente se diferenciará del revocado en el OID de la política que le aplica, para reflejar los cambios.

#### 9.11.2.Procedimientos de publicación y notificación.

Toda modificación de esta Declaración de Prácticas de Certificación o de los Documentos de Políticas de Certificación se publicará en el sitio web de la ACEDICOM.

#### 9.11.3.Procedimientos de aprobación de la Declaración de Prácticas de Certificación

La Dirección Técnica de EDICOM es la entidad competente para acordar la aprobación de la presente Declaración de Prácticas de Certificación, así como de las Políticas de Certificación asociadas a cada tipo de certificado.

Asimismo compete a la Dirección Técnica de EDICOM la aprobación y autorización de las modificaciones de dichos documentos.

### 9.12.RESOLUCIÓN DE CONFLICTOS.

#### 9.12.1.Resolución extrajudicial de conflictos.

La ACEDICOM podrá establecer, a través de los instrumentos jurídicos mediante los que se articule su relación con suscriptores y verificadores, los procedimientos de mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo.

#### 9.12.2.Jurisdicción competente.

La ACEDICOM establece, en sus instrumentos jurídicos con suscriptores y verificadores, los procedimientos de mediación y resolución de conflictos aplicables.

### 9.13.LEGISLACIÓN APLICABLE

El funcionamiento y operaciones de ACEDICOM, así como la presente CPS están regidos por la legislación comunitaria y estatal vigente en cada momento.

Explícitamente se asumen como de aplicación las siguientes normas:

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.
- La Directiva 11999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

### 9.14.CONFORMIDAD CON LA LEY APLICABLE

La ACEDICOM declara que la presente CPS cumple con las prescripciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

## 9.15. CLÁUSULAS DIVERSAS.

Sin estipulación adicional.