



Política de Certificación de Certificados Reconocidos de firma con limitación uso sobre soporte software

Fecha: 18/12/09 **Versión:** 1.2

Estado: VIGENTE **Nº de páginas:**

OID: 1.3.6.1.4.1.30051.2.1.2.5.2 **Clasificación:** PUBLICO

Archivo: ACEDICOM - Política FirmaAtributosSoft

Preparado por: Autoridad de Certificación EDICOM - ACEDICOM

Versión	Fecha	Descripción	Páginas
V 1.0	24/09/09	Documento inicial	
V 1.1	18/12/09	Cambio de la vigencia del certificado a 2 años Cambio de OID del documento Aclaración de campos a rellenar según tipo de persona física o jurídica	

Índice de contenido

1. INTRODUCCIÓN.....	8
1.1. PRESENTACIÓN.....	8
1.2. IDENTIFICACIÓN.....	9
1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN.....	9
1.3.1. Autoridades de Certificación.....	9
1.3.2. Autoridades de Registro.....	9
1.3.3. Usuarios Finales.....	9
1.4. USO DE LOS CERTIFICADOS.....	9
1.4.1. Usos Permitidos.....	9
1.4.2. Usos prohibidos.....	11
1.4.3. Fiabilidad de la firma electrónica a lo largo del tiempo.....	11
1.5. POLÍTICA DE ADMINISTRACIÓN.....	11
1.5.1. Especificación de la Organización Administradora.....	11
1.5.2. Persona de Contacto.....	11
1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas.....	12
1.6. DEFINICIONES Y ACRÓNIMOS.....	12
1.6.1. Definiciones.....	12
1.6.2. Acrónimos.....	12
2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS.....	13
2.1. REPOSITORIO DE CERTIFICADOS.....	13
2.2. PUBLICACIÓN.....	13
2.3. FRECUENCIA DE ACTUALIZACIONES.....	13
2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.....	13
3. IDENTIFICACIÓN Y AUTENTICACIÓN.....	14
3.1. REGISTRO DE NOMBRES.....	14
3.1.1. Tipos de nombres.....	14
3.1.2. Significado de los nombres.....	14
3.1.3. Interpretación de formatos de nombres.....	14
3.1.4. Unicidad de los nombres.....	14
3.1.5. Resolución de conflictos relativos a nombres.....	14
3.1.6. Reconocimiento, autenticación y función de las marcas registradas.....	14
3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD.....	14
3.2.1. Métodos de prueba de posesión de la clave privada.....	14
3.2.2. Autenticación de la identidad de una organización.....	14
3.2.3. Autenticación de la identidad de un individuo.....	14
3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE.....	14
3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.....	14
3.3.2. Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida.....	15
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE.....	15
4. EL CICLO DE VIDA DE LOS CERTIFICADOS.....	16
4.1. SOLICITUD DE CERTIFICADOS.....	16
4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.....	16
4.3. EMISIÓN DE CERTIFICADOS.....	16
4.4. ACEPTACIÓN DE CERTIFICADOS.....	16
4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.....	16
4.6. RENOVACIÓN DE CERTIFICADOS.....	17

4.7. RENOVACIÓN DE CLAVES.....	17
4.8. MODIFICACIÓN DE CERTIFICADOS.....	17
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	17
4.9.1. Circunstancias para la revocación.....	17
4.9.2. Entidad que puede solicitar la revocación.....	17
4.9.3. Procedimiento de solicitud de revocación.....	17
4.9.4. Periodo de gracia de la solicitud de revocación.....	17
4.9.5. Circunstancias para la suspensión.....	17
4.9.6. Entidad que puede solicitar la suspensión.....	17
4.9.7. Procedimiento para la solicitud de suspensión.....	17
4.9.8. Límites del período de suspensión.....	17
4.9.9. Frecuencia de emisión de CRLs.....	17
4.9.10. Requisitos de comprobación de CRLs.....	17
4.9.11. Disponibilidad de comprobación on-line de revocación y estado.....	17
4.9.12. Requisitos de comprobación on-line de revocación.....	17
4.9.13. Otras formas de divulgación de información de revocación disponibles.....	18
4.9.14. Requisitos de comprobación para otras formas de divulgación de información de revocación.....	18
4.9.15. Requisitos especiales de renovación de claves comprometidas.....	18
4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.....	18
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN.....	18
4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES.....	18
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.....	19
5.1. CONTROLES DE SEGURIDAD FÍSICA.....	19
5.1.1. Ubicación y construcción.....	19
5.1.2. Acceso físico.....	19
5.1.3. Alimentación eléctrica y aire acondicionado.....	19
5.1.4. Exposición al agua.....	19
5.1.5. Protección y prevención de incendios.....	19
5.1.6. Sistema de almacenamiento.....	19
5.1.7. Eliminación de residuos.....	19
5.1.8. Backup remoto.....	19
5.2. CONTROLES DE PROCEDIMIENTOS.....	19
5.2.1. Papeles de confianza.....	19
5.2.2. Número de personas requeridas por tarea.....	19
5.2.3. Identificación y autenticación para cada papel.....	19
5.3. CONTROLES DE SEGURIDAD DE PERSONAL.....	19
5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación.....	19
5.3.2. Procedimientos de comprobación de antecedentes.....	20
5.3.3. Requerimientos de formación.....	20
5.3.4. Requerimientos y frecuencia de actualización de la formación.....	20
5.3.5. Frecuencia y secuencia de rotación de tareas.....	20
5.3.6. Sanciones por acciones no autorizadas.....	20
5.3.7. Requerimientos de contratación de personal.....	20
5.3.8. Documentación proporcionada al personal.....	20
5.3.9. Controles periódicos de cumplimiento.....	20
5.3.10. Finalización de los contratos.....	20
5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....	20
5.4.1. Tipos de eventos registrados.....	20
5.4.2. Frecuencia de procesado de logs.....	20
5.4.3. Periodo de retención para los logs de auditoría.....	20
5.4.4. Protección de los logs de auditoría.....	20
5.4.5. Procedimientos de backup de los logs de auditoría.....	20
5.4.6. Sistema de recogida de información de auditoría (interno vs externo).....	20

5.4.7. Notificación al sujeto causa del evento.....	21
5.4.8. Análisis de vulnerabilidades.....	21
5.5. ARCHIVO DE INFORMACIONES Y REGISTROS.....	21
5.5.1. Tipo de informaciones y eventos registrados.....	21
5.5.2. Periodo de retención para el archivo.....	21
5.5.3. Protección del archivo.....	21
5.5.4. Procedimientos de backup del archivo.....	21
5.5.5. Requerimientos para el sellado de tiempo de los registros.....	21
5.5.6. Sistema de recogida de información de auditoría (interno vs externo).....	21
5.5.7. Procedimientos para obtener y verificar información archivada.....	21
5.6. CAMBIO DE CLAVE.....	21
5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE.....	21
5.7.1. Alteración de los recursos hardware, software y/o datos.....	21
5.7.2. La clave pública de una entidad se revoca.....	21
5.7.3. La clave de una entidad se compromete.....	22
5.7.4. Instalación de seguridad después de un desastre natural u otro tipo de desastre.....	22
5.8. CESE DE UNA CA.....	22
6. CONTROLES DE SEGURIDAD TÉCNICA.....	23
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	23
6.1.1. Generación del par de claves.....	23
6.1.2. Entrega de la clave privada a la entidad.....	23
6.1.3. Entrega de la clave pública al emisor del certificado.....	23
6.1.4. Entrega de la clave pública de la CA a los usuarios.....	23
6.1.5. Tamaño de las claves.....	23
6.1.6. Parámetros de generación de la clave pública.....	23
6.1.7. Comprobación de la calidad de los parámetros.....	23
6.1.8. Hardware/software de generación de claves.....	24
6.1.9. Fines del uso de la clave.....	24
6.2. PROTECCIÓN DE LA CLAVE PRIVADA.....	24
6.2.1. Estándares para los módulos criptográficos.....	24
6.2.2. Control multipersona de la clave privada.....	24
6.2.3. Custodia de la clave privada.....	24
6.2.4. Copia de seguridad de la clave privada.....	24
6.2.5. Archivo de la clave privada.....	24
6.2.6. Introducción de la clave privada en el módulo criptográfico.....	25
6.2.7. Método de activación de la clave privada.....	25
6.2.8. Método de desactivación de la clave privada.....	25
6.2.9. Método de destrucción de la clave privada.....	25
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	25
6.3.1. Archivo de la clave pública.....	25
6.3.2. Periodo de uso para las claves públicas y privadas.....	25
6.4. DATOS DE ACTIVACIÓN.....	25
6.4.1. Generación y activación de los datos de activación.....	25
6.4.2. Protección de los datos de activación.....	25
6.4.3. Otros aspectos de los datos de activación.....	25
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA.....	26
6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	26
6.7. CONTROLES DE SEGURIDAD DE LA RED.....	26
6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS.....	26
7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS.....	27
7.1. PERFIL DE CERTIFICADO.....	27
7.1.1. Número de versión.....	27
7.1.2. Extensiones del certificado.....	27

7.1.3. Identificadores de objeto (OID) de los algoritmos.....	30
7.1.4. Formatos de nombres.....	30
7.1.5. Restricciones de los nombres.....	31
7.1.6. Identificador de objeto (OID) de la Política de Certificación.....	31
7.1.7. Uso de la extensión “Policy Constraints”.....	31
7.1.8. Sintaxis y semántica de los cualificadores de política.....	31
7.1.9. Tratamiento semántico para la extensión crítica “Certificate Policy”.....	31
7.2. PERFIL DE CRL.....	31
7.2.1. Número de versión.....	31
7.2.2. CRL y extensiones.....	31
7.3 LISTAS DE CERTIFICADOS REVOCADOS.....	31
7.3.1 Limite Temporal de los certificados en las CRLs.....	31
7.4.- PERFIL DE OCSP.....	31
8. AUDITORÍA DE CONFORMIDAD.....	32
8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD.....	32
8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	32
8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	32
8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD.....	32
8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.....	32
8.6. COMUNICACIÓN DE RESULTADOS.....	32
9. REQUISITOS COMERCIALES Y LEGALES.....	33
9.1. TARIFAS.....	33
9.1.1. Tarifas de emisión de certificado o renovación.....	33
9.1.2. Tarifas de acceso a los certificados.....	33
9.1.3. Tarifas de acceso a la información de estado o revocación.....	33
9.1.4. Tarifas de otros servicios como información de políticas.....	33
9.1.5. Política de reintegros.....	33
9.2. CAPACIDAD FINANCIERA.....	33
9.2.1. Indemnización a los terceros que confían en los certificados emitidos por la ACEDICOM.....	33
9.2.2. Relaciones fiduciarias.....	33
9.2.3. Procesos administrativos.....	33
9.3. POLÍTICA DE CONFIDENCIALIDAD.....	33
9.3.1. Información confidencial.....	33
9.3.2. Información no confidencial.....	33
9.3.3. Divulgación de información de revocación /suspensión de certificados.....	33
9.4. PROTECCIÓN DE DATOS PERSONALES.....	34
9.4.1. Plan de Protección de Datos Personales.....	34
9.4.2. Información considerada privada.....	34
9.4.3. Información no considerada privada.....	34
9.4.4. Responsabilidades.....	34
9.4.5. Prestación del consentimiento en el uso de los datos personales.....	34
9.4.6. Comunicación de la información a autoridades administrativas y/o judiciales.....	34
9.4.7. Otros supuestos de divulgación de la información.....	34
9.5. DERECHOS DE PROPIEDAD INTELECTUAL.....	34
9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL.....	34
9.6.1. Obligaciones de la Entidad de Certificación.....	34
9.6.2. Obligaciones de la Autoridad de Registro.....	34
9.6.3. Obligaciones de los suscriptores.....	34
9.6.4. Obligaciones de los terceros confiantes en los certificados emitidos por la ACEDICOM.....	34
9.6.5. Obligaciones del repositorio.....	34
9.7. RENUNCIAS DE GARANTÍAS.....	35
9.8. LIMITACIONES DE RESPONSABILIDAD.....	35
9.8.1. Garantías y limitaciones de garantías.....	35

9.8.2. Deslinde de responsabilidades.....	35
9.8.3. Limitaciones de pérdidas.....	35
9.9. PLAZO Y FINALIZACIÓN.....	35
9.9.1. Plazo.....	35
9.9.2. Finalización.....	35
9.9.3. Supervivencia.....	35
9.10. NOTIFICACIONES.....	35
9.11. MODIFICACIONES.....	35
9.11.1. Procedimientos de especificación de cambios.....	35
9.11.2. Procedimientos de publicación y notificación.....	35
9.11.3. Procedimientos de aprobación de la Declaración de Prácticas de Certificación.....	35
9.12. RESOLUCIÓN DE CONFLICTOS.....	35
9.12.1. Resolución extrajudicial de conflictos.....	36
9.12.2. Jurisdicción competente.....	36
9.13. LEGISLACIÓN APLICABLE.....	36
9.14. CONFORMIDAD CON LA LEY APLICABLE.....	36
9.15. CLÁUSULAS DIVERSAS.....	36

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”*

El presente documento es la Política de Certificación asociada a los **certificados reconocidos de firma con limitación de uso sobre dispositivo software**, que contiene las reglas a las que se sujeta el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Autoridad de Certificación EDICOM (ACEDICOM) y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la *Declaración de Prácticas de Certificación (CPS)* de la ACEDICOM.

La Política de Certificación referida en este documento se utilizará para la emisión de certificados reconocidos de firma sobre dispositivo software para ser utilizados dentro del ámbito general de las aplicaciones de firma electrónica.

Estos certificados son compatibles con las especificaciones técnicas del apartado tercero de la Orden Ministerial HAC /1181/2003, de 12 de Mayo por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.

Este tipo de certificados se expiden con un periodo de vigencia de 2 años.

Mediante los certificados reconocidos en dispositivo software asociados a esta Política de Certificación se generarán firmas electrónicas avanzadas según la Directiva 1999/93/CE y la Ley 59/2003 de Firma Electrónica.

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 la ETSI TS 101 456 V1.2.1 *“Policy Requirements for certification authorities issuing qualified certificates”*, al igual que la Declaración de Prácticas de Certificación, para facilitar la lectura o comparación con documentos homólogos.

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

Esta Política de Certificación asume que el lector conoce los conceptos básicos de Infraestructura de Clave Pública, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2. IDENTIFICACIÓN

Nombre del documento	Política de Certificación de Certificados reconocidos de firma con limitación de uso en dispositivo software
Calificador de la política:	Certificado reconocido expedido por la ACEDICOM
Versión del documento	V 1.2
Estado del documento	Vigente
OID (Object Identifier)	1.3.6.1.4.1.30051.2.1.2.5.2
Fecha de emisión	18 de Diciembre de 2009
Fecha de expiración	No aplicable.
CPS relacionada	Declaración de Prácticas de Certificación (CPS) de la ACEDICOM. Versión 1.5 OID: 1.3.6.1.4.1.30051.2.1.1.1 Disponible en : http://acedicom.edicomgroup.com
Localización	http://acedicom.edicomgroup.com

1.3. COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN

1.3.1. Autoridades de Certificación

La CA que puede emitir certificados acordes con esta política es "ACEDICOM".

1.3.2. Autoridades de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

1.3.3. Usuarios Finales

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos Permitidos

Los certificados emitidos por la ACEDICOM bajo esta Política de Certificación son certificados reconocidos de firma electrónica y pueden utilizarse en aplicaciones que requieran el uso de esta tecnología con la limitación de uso por razón de ámbito que se establezca en la extensión

1.3.6.1.4.1.30051.3.1.2 de forma textual, publicándose las limitaciones posibles en el apartado “Limitaciones de uso” de ésta política de certificación en la web de la ACEDICOM <http://acedicom.edicomgroup.com> . En todo caso es el Solicitante del certificado el responsable del cumplimiento del ámbito de uso permitido con las limitaciones establecidas.

Las limitaciones de uso aceptadas para los certificados reconocidos de firma con limitación de uso sobre soporte software de la ACEDICOM se muestran en la siguiente tabla:

Etiqueta	Descripción
Control de acceso	Se utiliza para la identificación del usuario frente a un acceso de tipo físico o lógico
Firma de documentos comerciales y tributarios (pedidos, albaranes, facturas, etc.)	Se utiliza para el intercambio electrónico de documentos en las relaciones comerciales entre empresas privadas o públicas y en ámbito tributario

Este certificado (**certificado cualificado** según ETSI, la RFC3739 y la Directiva Europea 99/93/EC. y **reconocido** según la ley de Firma Electrónica) permite la generación de firmas electrónicas avanzadas.

Los certificados de firma con limitación de uso 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 artículo 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

El uso de estos certificados proporciona 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 este certificado se emite sobre dispositivo seguro 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.

- El uso de este certificado, no significa que se esté dando el acuerdo sobre el contenido del documento firmado.

1.4.2. Usos prohibidos

Los certificados se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y con arreglo a la normativa vigente.

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 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. POLÍTICA DE ADMINISTRACIÓN

1.5.1. Especificación de la Organización Administradora

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

1.5.2. Persona de Contacto

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

1.5.3. Competencia para determinar la adecuación de la CPS a la Políticas

La Dirección Técnica de EDICOM es el Órgano competente para determinar la adecuación de esta Política de Certificación a la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

No estipulado

1.6.2. Acrónimos

No estipulado

2. PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1. REPOSITORIO DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

2.2. PUBLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

2.3. FRECUENCIA DE ACTUALIZACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

2.4. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

Las especificaciones contenidas en este apartado complementan estipulaciones previstas la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM en caso de ser necesario.

3.1. REGISTRO DE NOMBRES

3.1.1. Tipos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.1.2. Significado de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.1.3. Interpretación de formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.1.4. Unicidad de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.1.5. Resolución de conflictos relativos a nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

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

Los pares de claves asociados a los certificados de esta política se generan mediante un proceso controlado en todo momento por el solicitante utilizando un dispositivo software, normalmente el propio navegador de internet. Es el propio usuario el que debe garantizar que en todo momento las claves privadas están bajo su control no utilizando equipos compartidos y mediante la correspondiente protección del mismo mediante mecanismos basados en usuario y contraseña. Las claves privadas se generan en el dispositivo software del suscriptor y pueden ser exportadas, proceso que el suscriptor deberá proteger mediante el uso de contraseña en el archivo exportado.

3.2.2. Autenticación de la identidad de una organización.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.2.3. Autenticación de la identidad de un individuo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4. EL CICLO DE VIDA DE LOS CERTIFICADOS.

Las especificaciones contenidas en este apartado complementan estipulaciones previstas en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM en caso de ser necesario.

4.1. SOLICITUD DE CERTIFICADOS

La entidad o persona que desee le sea emitido un certificado de acuerdo con esta política de certificación deberá solicitarlo a través del documento “CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL” que puede obtener en la página web de la ACEDICOM <http://acedicom.edicomgroup.com> en el Área “Gestion de Certificados”.

En el momento de formalizar su solicitud, el solicitante deberá acreditar su identidad de forma presencial o remota ante cualquier Punto de registro autorizado, tal como se describe en la CPS (Declaración de Prácticas de Certificación) punto 3.2.3, presentar el “CONTRATO DE PRESTACION DE SERVICIOS DE CERTIFICACION DIGITAL” debidamente firmado y, en su caso, la documentación que corresponda con arreglo al tipo de entidad y representación tal como se indica en el CPS punto 3.2.2.

A estos efectos se podrá prescindir de la presencia física si la firma contenida en el Contrato ha sido legitimada notarialmente.

El encargado de recibir dicha documentación en la Entidad de Registro, comprobará la identidad del solicitante y verificará los documentos acreditativos de su representación así como su inscripción en el correspondiente registro público, si resultara exigible.

Hechas todas estas comprobaciones se valida la solicitud en el sistema informático enviándola electrónicamente y de forma segura a la ACEDICOM. En el caso de denegación de la solicitud de certificación por parte del Operador de la Autoridad de Registro, el solicitante recibirá información de los motivos del rechazo de la misma.

Obtenido/s el/los certificado/s el solicitante recibirá una notificación por Email de los detalles y atributos del/os mismo/s.

El listado de Puntos de registro autorizados se encuentra en la página web <http://acedicom.edicomgroup.com> en el Área “Puntos de Registro”.

4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.3. EMISIÓN DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.4. ACEPTACIÓN DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.

Los certificados ACEDICOM bajo esta política son certificados reconocidos de firma para el ámbito general, destinados a personas físicas o a entidades jurídicas (colectivamente llamados suscriptores).

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

4.6. RENOVACIÓN DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.7. RENOVACIÓN DE CLAVES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.8. MODIFICACIÓN DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.

4.9.1. Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.2. Entidad que puede solicitar la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.3. Procedimiento de solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.4. Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.5. Circunstancias para la suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.6. Entidad que puede solicitar la suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.7. Procedimiento para la solicitud de suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.8. Límites del período de suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.9. Frecuencia de emisión de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.10. Requisitos de comprobación de CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.11. Disponibilidad de comprobación on-line de revocación y estado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.12. Requisitos de comprobación *on-line* de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.13. Otras formas de divulgación de información de revocación disponibles

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.14. Requisitos de comprobación para otras formas de divulgación de información de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.9.15. Requisitos especiales de renovación de claves comprometidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.10. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

4.12. DEPÓSITO Y RECUPERACIÓN DE CLAVES.

La ACEDICOM no realiza en este caso el depósito de claves de firma, si no que éstas se generan en el dispositivo software que está en poder exclusivo del propio suscriptor.

Las claves privadas pueden ser exportables y deben ser protegidas por el usuario mediante mecanismos del tipo "palabra de clave".

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

5.1. CONTROLES DE SEGURIDAD FÍSICA

5.1.1. Ubicación y construcción

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.2. Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.3. Alimentación eléctrica y aire acondicionado

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.4. Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.5. Protección y prevención de incendios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.6. Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.7. Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.1.8. Backup remoto

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.2. CONTROLES DE PROCEDIMIENTOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.2.1. Papeles de confianza

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.2.2. Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.2.3. Identificación y autenticación para cada papel

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3. CONTROLES DE SEGURIDAD DE PERSONAL

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.6. Sanciones por acciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.7. Requerimientos de contratación de personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.9. Controles periódicos de cumplimiento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.3.10. Finalización de los contratos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

5.4.1. Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4.2. Frecuencia de procesado de logs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4.3. Periodo de retención para los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4.4. Protección de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4.5. Procedimientos de backup de los logs de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4.7. Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.4.8. Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.5. ARCHIVO DE INFORMACIONES Y REGISTROS

5.5.1. Tipo de informaciones y eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.5.2. Periodo de retención para el archivo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.5.3. Protección del archivo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.5.4. Procedimientos de backup del archivo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.5.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.6. CAMBIO DE CLAVE

No estipulado.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.7.2. La clave pública de una entidad se revoca

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.7.3. La clave de una entidad se compromete

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

5.8. CESE DE UNA CA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.1 de la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.1.1. Generación del par de claves

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en el dispositivo software que está bajo el control del propio suscriptor, normalmente un navegador de internet. Los únicos que tienen acceso a las claves de firma son los propietarios de las mismas mediante la posesión y protección del equipo que realiza la petición.

Las claves privadas pueden ser exportables y deben ser protegidas por el usuario mediante mecanismos del tipo “palabra de clave”.

6.1.2. Entrega de la clave privada a la entidad

La clave privada se genera mediante un proceso iniciado por el propio titular en el dispositivo software que obra en su poder. No existe por tanto ninguna transferencia de clave privada.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada en el interior del dispositivo criptográfico software en poder del suscriptor y es enviada a la PKI ACEDICOM formando parte de una solicitud 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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.1.5. Tamaño de las claves

El tamaño de las claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación es de 2048 bits mínimo.

6.1.6. Parámetros de generación de la clave pública

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI SR 002 176 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature”.

Signature algorithm Signature algorithm parameters

Rsa MinModLen=1020

Key generation algorithm

rsagen1

Padding method Cryptographic

emsa-pkcs1-v1_5

Hash function

sha1

6.1.7. Comprobación de la calidad de los parámetros

Se utilizan los parámetros definidos en la suite criptográfica 001 especificada en el documento de ETSI SR 002 176 “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signature”.

6.1.8. Hardware/software de generación de claves

El par de claves se generan en el dispositivo software que está en poder exclusivo del propio suscriptor. Los únicos que tienen acceso a las claves de firma son los propietarios de las mismas mediante la posesión y protección del equipo que las alberga. Las claves privadas pueden ser exportables y deben ser protegidas por el usuario mediante mecanismos del tipo “palabra de clave”.

6.1.9. Fines del uso de la clave

Las claves definidas por la presente política se utilizarán para usos descritos en el punto de este documento *1.3 Comunidad de usuarios y ámbito de aplicación*.

La definición detallada del perfil de certificado y los usos de las claves se encuentra en el apartado 7 de este documento *“Perfiles de certificado y listas de certificados revocados”*.

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

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en el punto 6.2 de la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.2.1. Estándares para los módulos criptográficos

El dispositivo criptográfico seguro empleado en la emisión de los certificados adscritos a esta Política de Certificación dispone de certificación CC EAL4+ y CWA 14169.

6.2.2. Control multipersona de la clave privada

Las claves privadas para los certificados de firma emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores del mismo.

6.2.3. Custodia de la clave privada

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores del mismo, por lo tanto la ACEDICOM no realiza ningún tipo de custodia sobre las claves privadas asociadas a esta política.

6.2.4. Copia de seguridad de la clave privada

Las claves privadas pueden ser exportables y deben ser protegidas por el usuario mediante mecanismos del tipo “palabra de clave”.

6.2.5. Archivo de la clave privada.

Las claves privadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los suscriptores de los mismos. Las claves privadas pueden ser exportables y deben ser protegidas por el usuario mediante mecanismos del tipo “palabra de clave”.

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

La generación de las claves vinculadas al certificado de firma se realiza dentro del dispositivo software del usuario. Las claves privadas pueden ser exportables y deben ser protegidas por el usuario mediante mecanismos del tipo “palabra de clave”. Se podrían importar en otro dispositivo software siempre que se conozca dicha “palabra clave”.

6.2.7. Método de activación de la clave privada.

La activación de la clave privada se realizará a través de la introducción de la palabra de paso de acceso a esta clave, contenida en el fichero PKCS#12.

6.2.8. Método de desactivación de la clave privada

La desactivación se realizará cerrando la aplicación que la utiliza o cerrando el módulo criptográfico asociado.

6.2.9. Método de destrucción de la clave privada

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

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

6.3.1. Archivo de la clave pública

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.3.2. Periodo de uso para las claves públicas y privadas

Los certificados emitidos al amparo de la presente política tienen una validez de cuatro (4) años. El par de claves utilizado para la emisión de los certificados se crea para cada emisión, y por tanto también tienen una validez de cuatro (4) años.

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

Es el propio suscriptor el que genera el par de claves en el dispositivo software. Es responsabilidad y obligación del suscriptor el control de sus claves.

6.4.2. Protección de los datos de activación

El suscriptor del certificado es el responsable de la protección de los datos de activación de su clave privada.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.7. CONTROLES DE SEGURIDAD DE LA RED

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

6.8. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

7.1. PERFIL DE CERTIFICADO

7.1.1. Número de versión

Los certificados de identidad pública emitidos por la AC Subordinada utilizan el estándar X.509 versión 3 (X.509 v3)

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.
- *LimitaciónDeUso* (1.3.6.1.4.1.30051.3.1.2). Calificada como no crítica
- *NIF del responsable* (AEAT, 1.3.6.1.4.1.18838.1.1). No crítica

Los certificados emitidos bajo esta política se pueden emitir a:

•Personas físicas: se rellenan todos los campos del certificados salvo el de NIF del responsable (AEAT, 1.3.6.1.4.1.18838.1.1). El campo de Organización (O) es opcional para el caso de personas físicas pero si se rellena es informativo de la organización en la que trabaja y hay que comprobarlo.

•Personas jurídicas: se rellenan todos los campos incluido el NIF del responsable (AEAT, 1.3.6.1.4.1.18838.1.1), que será el código de identificación fiscal de la empresa. En el campo CN se pondrá el nombre de la persona jurídica mientras que en el SN,GN y S el NIF, nombre y apellidos respectivamente del representante persona física del certificado.

El perfil de los certificados emitidos bajo esta política son:

Campo	Contenido	I	C	T
Versión	v3	S		F
Serial Number	Asignado automáticamente por la AC	S		F
Signature Algorithm	SHA1withRSAEncryption	S		F
Issuer Distinguished Name	CN=ACEDICOM XX, OU=PKI, O=EDICOM, C=ES	S		F
Validez	2 años	S		F
Subject Public Key Info	Tipo de clave: RSA Longitud de la clave: 2048 bits	S		F
Subject		S		D
CommonName (CN)	Titular del certificado o Razón Social en personas jurídicas	S		D
SerialNumber (SN)	NIF del titular del certificado	S		D
GivenName (GN)	Nombre propio del responsable según DNI	S		D
Surname (S)	Apellidos del responsable según DNI	S		D
DN Qualifier	Código de identificación unívoco asignado por el emisor del certificado.	S		D

Country (C)	País de la organización (no tiene por qué coincidir con la nacionalidad del sujeto)	S		D
NIF del responsable 1.3.6.1.4.1.18838.1.1	NIF del responsable . Sólo en caso de personas jurídicas	C		D
Subject Alternative Names				
E-Mail (RFC 822)	Dirección de E-Mail del sujeto	O		D
SubjectKeyIdentifier	Identificador de la clave pública del certificado	S		D
AuthorityKeyIdentifier	Identificador de la clave pública asociada a la clave privada de la CA usada para firmar el presente certificado	S		F
BasicConstraints		S	X	F
CA	Falso	S	X	F
pathLength	No aplicable (0)			F
KeyUsage	digitalSignature	S	X	F
Certificate Policies		S		F
policyIdentifier	1.3.6.1.4.1.30051.2.1.2.5.2	S		F
CPSuri	http://acedicom.edicomgroup.com	S		F
policyIdentifier	1.3.6.1.4.1.30051.2.1.2.5.2	S		F
userNotice	Certificate Policy for Qualified Certificates for signing with usage limitation	S		F
policyIdentifier	QCP Public (0.4.0.1456.1.2)	S		F
LimitaciónDeUso 1.3.6.1.4.1.30051.3.1.2	Según tabla			
ExtendedKeyUsage	- no aplica -	C		F
CRLDistributionPoints		S		F
distributionPoint	http://acedicom.edicomgroup.com/acedicomXX.crl	S		F
Authority Information Access		S		F
accessMethod	Calssuers (indicamos la información de revocación de la CA que emitió el certificado de la CA emisora del presente certificado)	S		F
AccessLocation	http://www.edicomgrup.com/acedicom/certs/rootca.cer	S		F
accessMethod	OCSP	S		F
AccessLocation	http://ocspXX.acedicom.edicomgroup.com/	S		F
QC Statements (id-pe-qcStatements)		S		F
QCSyntax-v2	- Presente -	S		F
QCRetentionPeriod	13	S		F
ETSI QcCompliance	- Presente -	S		F

Leyenda de la tabla:

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

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.

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

- El Número de Serie del certificado al representarse en notación hexadecimal no superará los 32 caracteres hexadecimales.
- El Número de Serie más el contenido de Emisor del certificado no superará los 247 bytes.

Los certificados emitidos bajo esta política se emiten en calidad de certificados reconocidos y, por tanto este perfil contiene los campos que establece la normativa legalmente aplicable en materia de Certificados Reconocidos:

**Artículo 11 del Capítulo II de la ley de firma 59/2003 de 19 Dic.
 Anexo I de la Directiva del Parlamento Europeo 1999/93/EC**

Requisitos Legales	Modo de cumplimiento
La indicación que se expiden como certificados reconocidos (artículo 11.2.a 59/2003)	Inclusión de la extensión Qualified Certificate Statements que incorpora las siguientes declaraciones: 1.- id-etsi-qcs-QcCompliance – Indica que el certificado se emite como reconocido de acuerdo a los Anexo I y II de la Directiva del Parlamento Europeo 1999/93/EC y a la ley 59/2003, de 19 de diciembre, de firma electrónica.
La identificación del prestador de servicios de certificación que expide el certificado y el país en el que está establecido (artículo 11.2.c 59/2003)	A través de la información que se recoge en el campo Issuer del certificado tal y como contempla la rfc 3739 En el certificado se recoge claramente el país en el que se establece el PSC en el atributo Country del DN del campo Issuer En la presente política referenciadas en el certificado, se recoge el nombre o razón social, domicilio, dirección electrónica y número de identificación fiscal de la Institución que actúa como PSC de la ACEDICOM: EDICOM.
La identificación del firmante (el suscriptor del certificado), por su nombre y apellidos y DNI o equivalente, o a través de un seudónimo que conste de manera inequívoca. (artículo 11.2.e 59/2003)	A través de la información que se recoge en el campo Subject del certificado tal y como contempla la rfc 3739: Nombre, Apellidos y DNI. También organización que representa y CIF de la organización Se contempla la inclusión de la extensión Subject Alternative Names para indicar el email de contacto
La inclusión de algún atributo del firmante (el subscriptor), relevante para el uso establecido para el certificado en la Política. (artículo 11.3 59/2003)	Se incluye dentro del Subject un OID específico (1.3.6.1.4.1.18838.1.1) para indicar el CIF de la organización representada
Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante. (artículo 11.2.f 59/2003)	La clave pública del suscriptor se encuentra en el certificado tal y como contempla la RFC 3280. (Subject Public Key Info)
El comienzo y el final del periodo de validez del certificado. (artículo 11.2.g 59/2003)	El periodo de validez de las claves y el certificado asociado se encuentra recogido en el campo del certificado contemplado en la ITU-T Recommendation X.509 y en RFC 3280

El código identificativo único del certificado. (artículo 11.2.b 59/2003)	La pareja formada por el Número de serie del certificado y el Issuer tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 3280
La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado. (artículo 11.2.d 59/2003)	La firma digital del emisor del certificado de acuerdo con la ITU-T Recommendation X.509 y la RFC 3280
Los límites de uso del certificado, si se prevén. (artículo 11.2.h 59/2003)	Estos límites están reflejados en la Política de Certificación asociada a este certificados y en la extensión KeyUsage tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 3280. En este caso <i>digitalSignature</i> También se incluye el atributo <i>LímiteDeUso</i> (1.3.6.1.4.1.30051.3.1.2)
Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen. (artículo 11.2.i 59/2003)	No estipulado

**Artículos 18,19,20 del Capítulo II de la ley de firma 59/2003 de 19 Dic.
 Anexo II de la Directiva del Parlamento Europeo 1999/93/EC**

Requisitos Legales	Modo de cumplimiento
El requisito B) establece la necesidad de un servicio de comprobación del estado de los certificados. (artículo 18.d 59/2003)	La extensión AIA (Authority Information Access) contiene la URL del servicio de validación de certificados
El requisito i) establece un periodo mínimo de retención de la información relevante (artículo 20.1.f 59/2003)	En QCStatements se ha contemplado un periodo de 13 años adicionales a los 2 de vigencia del certificado, en total 15 años.
El requisito K) establece que los términos y condiciones de uso de los certificados deben estar accesibles a las terceras partes que hacen uso del certificado. (artículo II.19.2 59/2003)	En la extensión CertificatePolicies se indica la URL en la que están accesibles la DPC y las Políticas de Certificación asociadas al certificado

7.1.3. Identificadores de objeto (OID) de los algoritmos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

7.1.4. Formatos de nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

7.1.5. Restricciones de los nombres

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

El identificador de objeto definido por ACEDICOM para identificar la presente política es el siguiente: 1.3.6.1.4.1.30051.2.1.2.5.2

7.1.7. Uso de la extensión “Policy Constraints”

No se hace uso de la extensión “*Policy Constraints*” en los certificados emitidos bajo la presente Política de Certificación.

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.

Certificate Policies		S	F
policyIdentifier	1.3.6.1.4.1.30051.2.1.2.5.2	S	F
CPSuri	http://acedicom.edicomgroup.com	S	F
policyIdentifier	1.3.6.1.4.1.30051.2.1.2.5.2	S	F
userNotice	Certificate Policy for Qualified Certificates for digital signature located at http://acedicom.edicomgroup.com	S	F
policyIdentifier	QCP Public (0.4.0.1456.1.2)	S	F

7.2. PERFIL DE CRL

7.2.1. Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

7.2.2. CRL y extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

7.3 LISTAS DE CERTIFICADOS REVOCADOS

7.3.1 Limite Temporal de los certificados en las CRLs

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

7.4.- PERFIL DE OCSP

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

8. AUDITORÍA DE CONFORMIDAD

8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

8.6. COMUNICACIÓN DE RESULTADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. TARIFAS

9.1.1. Tarifas de emisión de certificado o renovación

La emisión de certificados digitales bajo la presente política de certificación está sometida a unas tarifas fijadas por EDICOM. Los precios públicos actualizados se recogen en la web de la ACEDICOM.

9.1.2. Tarifas de acceso a los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.1.4. Tarifas de otros servicios como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.1.5. Política de reintegros

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.2. CAPACIDAD FINANCIERA

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.2.2. Relaciones fiduciarias

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.2.3. Procesos administrativos

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.3. POLÍTICA DE CONFIDENCIALIDAD

9.3.1. Información confidencial.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.3.2. Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.3.3. Divulgación de información de revocación /suspensión de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.4. PROTECCIÓN DE DATOS PERSONALES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.4.1. Plan de Protección de Datos Personales.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.4.2. Información considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.4.3. Información no considerada privada.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.4.4. Responsabilidades.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.4.7. Otros supuestos de divulgación de la información.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM..

9.6. OBLIGACIONES Y RESPONSABILIDAD CIVIL

9.6.1. Obligaciones de la Entidad de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.6.2. Obligaciones de la Autoridad de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.6.3. Obligaciones de los suscriptores

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.6.5. Obligaciones del repositorio

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.7. RENUNCIAS DE GARANTÍAS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.8. LIMITACIONES DE RESPONSABILIDAD

9.8.1. Garantías y limitaciones de garantías

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.8.2. Deslinde de responsabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.8.3. Limitaciones de pérdidas

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.9. PLAZO Y FINALIZACIÓN.

9.9.1. Plazo.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.9.2. Finalización.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.9.3. Supervivencia.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.10. NOTIFICACIONES.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.11. MODIFICACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.11.1. Procedimientos de especificación de cambios

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.11.2. Procedimientos de publicación y notificación.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

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

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.12. RESOLUCIÓN DE CONFLICTOS.

9.12.1. Resolución extrajudicial de conflictos.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.12.2. Jurisdicción competente.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.13. LEGISLACIÓN APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.14. CONFORMIDAD CON LA LEY APLICABLE.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.

9.15. CLÁUSULAS DIVERSAS.

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de la ACEDICOM.