



# Política de Certificados TLS para cliente y servidor

**Fecha:** 15/01/10 **Versión:** V1.4  
**Estado:** VIGENTE **Nº de páginas:** 37  
**OID:** 1.3.6.1.4.1.30051.2.1.2.6.1 **Clasificación:** PÚBLICO  
**Archivo:** ACEDICOM - Politica Certificados TLS.odt  
**Preparado por:** Autoridad de Certificación EDICOM – ACEDICOM

### Historial de cambios

<b>Versión</b>	<b>Fecha</b>	<b>Descripción de la acción</b>	<b>Páginas / sección</b>
1.0	26/03/2009	Documento inicial	
1.1	20/01/2010	Mejoras derivadas de la revisión por Mozilla Foundation	
1.2	24/05/2010	Se contempla el uso extendido de claves para servicios de TimeStamp	
V1.3	17/09/10	Se documenta el uso de esta política para firma de documentos en entorno de proyectos	
V1.4	15/11/10	Se documenta el uso de esta política para la emisión de certificados de OFTP2	

# Tabla de Contenido

1	INTRODUCCIÓN	9
1.1	PRESENTACIÓN	9
1.2	IDENTIFICACIÓN	9
1.3	COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN	10
1.3.1	Autoridades de Certificación	10
1.3.2	Autoridades de Registro	10
1.3.3	Usuarios Finales	10
1.4	USO DE LOS CERTIFICADOS	10
1.4.1	Usos Permitidos	10
1.4.2	Usos prohibidos	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	11
1.6	DEFINICIONES Y ACRÓNIMOS	12
1.6.1	Definiciones	12
1.6.2	Acrónimos	12
2	PUBLICACIÓN DE INFORMACIONES 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	15
3.1.3	Interpretación de formatos de nombres	15
3.1.4	Unicidad de los nombres	15
3.1.5	Resolución de conflictos relativos a nombres	15
3.1.6	Reconocimiento, autenticación y función de las marcas registradas	15
3.1.7	Uso de comodines en los nombres	15
3.2	VERIFICACIÓN INICIAL DE LA IDENTIDAD	15
3.2.1	Métodos de prueba de posesión de la clave privada	15
3.2.2	Acreditación de identidad	16
3.2.2.1	Certificados de uso interno de ACEDICOM	17
3.3	IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE	17

3.3.1	Identificación y autenticación de las solicitudes de renovación rutinarias.	17
3.3.2	Identificación y autenticación de las solicitudes de renovación de clave después de una revocación – Clave no comprometida	17
3.4	IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE	17
4	EL CICLO DE VIDA DE LOS CERTIFICADOS	18
4.1	SOLICITUD DE CERTIFICADOS	18
4.2	TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS	18
4.3	EMISIÓN DE CERTIFICADOS	18
4.4	ACEPTACIÓN DE CERTIFICADOS	19
4.5	USO DEL PAR DE CLAVES Y DEL CERTIFICADO	19
4.6	RENOVACIÓN DE CERTIFICADOS	19
4.7	RENOVACIÓN DE CLAVES	19
4.8	MODIFICACIÓN DE CERTIFICADOS	19
4.9	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS	19
4.9.1	Circunstancias para la revocación	19
4.9.2	Entidad que puede solicitar la revocación	19
4.9.3	Procedimiento de solicitud de revocación	19
4.9.4	Periodo de gracia de la solicitud de revocación	19
4.9.5	Circunstancias para la suspensión	19
4.9.6	Entidad que puede solicitar la suspensión	20
4.9.7	Procedimiento para la solicitud de suspensión	20
4.9.8	Límites del período de suspensión	20
4.9.9	Frecuencia de emisión de CRLs	20
4.9.10	Requisitos de comprobación de CRLs	20
4.9.11	Otras formas de divulgación de información de revocación disponibles	20
4.9.12	Requisitos especiales de renovación de claves comprometidas	20
4.10	SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS	20
4.11	FINALIZACIÓN DE LA SUSCRIPCIÓN	20
4.12	DEPÓSITO Y RECUPERACIÓN DE CLAVES	20
5	CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES	21
5.1	CONTROLES DE SEGURIDAD FÍSICA	21
5.1.1	Ubicación y construcción	21
5.1.2	Acceso físico	21
5.1.3	Alimentación eléctrica y aire acondicionado	21
5.1.4	Exposición al agua	21
5.1.5	Protección y prevención de incendios	21
5.1.6	Sistema de almacenamiento	21
5.1.7	Eliminación de residuos	21
5.1.8	Backup remoto	21
5.2	CONTROLES DE PROCEDIMIENTOS	21
5.2.1	Papeles de confianza	21
5.2.2	Número de personas requeridas por tarea	22

5.2.3	Identificación y autenticación para cada papel	22
5.3	CONTROLES DE SEGURIDAD DE PERSONAL	22
5.3.1	Requerimientos de antecedentes, calificación, experiencia, y acreditación	22
5.3.2	Procedimientos de comprobación de antecedentes	22
5.3.3	Requerimientos de formación	22
5.3.4	Requerimientos y frecuencia de actualización de la formación	22
5.3.5	Frecuencia y secuencia de rotación de tareas	22
5.3.6	Sanciones por acciones no autorizadas	22
5.3.7	Requerimientos de contratación de personal	22
5.3.8	Documentación proporcionada al personal	22
5.3.9	Controles periódicos de cumplimiento	22
5.3.10	Finalización de los contratos	22
5.4	PROCEDIMIENTOS DE CONTROL DE SEGURIDAD	23
5.4.1	Tipos de eventos registrados	23
5.4.2	Frecuencia de procesado de logs	23
5.4.3	Periodo de retención para los logs de auditoría	23
5.4.4	Protección de los logs de auditoría	23
5.4.5	Procedimientos de backup de los logs de auditoría	23
5.4.6	Sistema de recogida de información de auditoría (interno vs externo)	23
5.4.7	Notificación al sujeto causa del evento	23
5.4.8	Análisis de vulnerabilidades	23
5.5	ARCHIVO DE INFORMACIONES Y REGISTROS	23
5.5.1	Tipo de informaciones y eventos registrados	23
5.5.2	Periodo de retención para el archivo	23
5.5.3	Protección del archivo	23
5.5.4	Procedimientos de backup del archivo	24
5.5.5	Requerimientos para el sellado de tiempo de los registros	24
5.5.6	Sistema de recogida de información de auditoría (interno vs externo)	24
5.5.7	Procedimientos para obtener y verificar información archivada	24
5.6	CAMBIO DE CLAVE	24
5.7	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE	24
5.7.1	Alteración de los recursos hardware, software y/o datos	24
5.7.2	La clave pública de una entidad se revoca	24
5.7.3	La clave de una entidad se compromete	24
5.7.4	Instalación de seguridad después de un desastre natural u otro tipo de desastre	24
5.8	CESE DE UNA CA	24
6	CONTROLES DE SEGURIDAD TÉCNICA	25
6.1	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	25
6.1.1	Generación del par de claves	25
6.1.2	Entrega de la clave privada a la entidad	25
6.1.3	Entrega de la clave pública al emisor del certificado	25
6.1.4	Entrega de la clave pública de la CA a los usuarios	25
6.1.5	Tamaño de las claves	25

6.1.6	Parámetros de generación de la clave pública	25
6.1.7	Comprobación de la calidad de los parámetros	26
6.1.8	Hardware/software de generación de claves	26
6.1.9	Fines del uso de la clave	26
6.2	PROTECCIÓN DE LA CLAVE PRIVADA	26
6.2.1	Estándares para los módulos criptográficos	26
6.2.2	Control multipersona de la clave privada	26
6.2.3	Custodia de la clave privada	26
6.2.4	Copia de seguridad de la clave privada	27
6.2.5	Archivo de la clave privada	27
6.2.6	Método de activación de la clave privada	27
6.2.7	Método de desactivación de la clave privada	27
6.2.8	Método de destrucción de la clave privada	27
6.3	OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES	27
6.3.1	Archivo de la clave pública	27
6.3.2	Periodo de uso para las claves públicas y privadas	27
6.4	DATOS DE ACTIVACIÓN	27
6.4.1	Generación y activación de los datos de activación	27
6.4.2	Protección de los datos de activación	28
6.4.3	Otros aspectos de los datos de activación	28
6.5	CONTROLES DE SEGURIDAD INFORMÁTICA	28
6.6	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	28
6.7	CONTROLES DE SEGURIDAD DE LA RED	28
6.8	CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS	28
7	PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS	29
7.1	PERFIL DE CERTIFICADO	29
7.1.1	Número de versión	29
7.1.2	Extensiones del certificado	29
7.1.3	Identificadores de objeto (OID) de los algoritmos	30
7.1.4	Formatos de nombres	31
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
7.2	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	34
9.3.3	Divulgación de información de revocación /suspensión de certificados	34
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	35
9.6.2	Obligaciones de la Autoridad de Registro	35
9.6.3	Obligaciones de los suscriptores	35
9.6.4	Obligaciones de los terceros confiantes en los certificados emitidos por la ACEDICOM	35
9.6.5	Obligaciones del repositorio	35
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	36
9.10 NOTIFICACIONES	36
9.11 MODIFICACIONES	36
9.11.1 Procedimientos de especificación de cambios	36
9.11.2 Procedimientos de publicación y notificación	36
9.11.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación	36
9.12 RESOLUCIÓN DE CONFLICTOS	36
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
Anexo I: Solicitud de revocación	37

# 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 TLS para cliente y servidor**, 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.

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

La citada 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.

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

<b>Nombre del documento</b>	Política de Certificados TLS para cliente y servidor
<b>Calificador de la política</b>	Certificado expedido por la ACEDICOM
<b>Versión del documento</b>	V1.4
<b>OID (Object Identifier)</b>	1.3.6.1.4.1.30051.2.1.2.6.1
<b>Fecha de emisión</b>	15/01/10
<b>Fecha de expiración</b>	No aplicable
<b>CPS relacionada</b>	Declaración de Prácticas de Certificación (CPS) de la ACEDICOM. Versión 1.4 OID: 1.3.6.1.4.1.30051.2.1.1.1 Disponible en: <a href="http://acedicom.edicomgroup.com">http://acedicom.edicomgroup.com</a>
<b>Localización</b>	<a href="http://acedicom.edicomgroup.com">http://acedicom.edicomgroup.com</a>

## 1.3 COMUNIDAD DE USUARIOS Y ÁMBITO DE APLICACIÓN

### 1.3.1 Autoridades de Certificación

La AC que puede emitir certificados acordes con esta política son "ACEDICOM Servidores", "ACEDICOM 01" y "ACEDICOM 02".

### 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 bajo el amparo de la presente política podrán usarse para facilitar la seguridad en las comunicaciones mediante el uso de cifrado SSL o TLS. Usos típicos de estos certificados pueden ser la autenticación (incluyendo *Active Directory* de Microsoft), cifrado de datos, firma electrónica de contenido, etc.

Los usos permitidos en el caso concreto de cada certificado se deducen de los valores de las extensiones *keyUsage* y *extendedKeyUsage* del certificado, con arreglo a lo estipulado en la RFC 3280 (<http://www.ietf.org/rfc/rfc3280.txt>) y esta política contempla:

- DE CLIENTE
  - Client Authentication (para validación web)
  - MS Smart Card Logon (OID 1.3.6.1.4.1.311.20.2.2), en tarjeta
  - Email Protection
  
- DE SERVIDOR
  - Server Authentication
  - Internet Key Exchange for IPSEC
  - Code signing
  - Timestamping
  - OFTP2 Server (Digitalsignature, KeyEncipherment, TLSServerAuthentication, TLSClientAuthentication). Se podrá elegir de dicha lista de 1 a 4 atributos en este tipo de certificados.

En concreto, los certificados emitidos bajo esta política podrán contener los siguientes valores en la extensión *extendedKeyUsage*:

- Server Authentication
- Client Authentication

- Email Protection
- MS Smart Card Logon (OID 1.3.6.1.4.1.311.20.2.2, consultar <http://support.microsoft.com/default.aspx?scid=kb;en-us;287547>)
- Internet Key Exchange for IPSEC
- Code signing
- TimeStamping

El perfil del certificado y las extensiones comentadas se desarrollan con más detalle en la sección 7.1.2.

## 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.

## 1.5 POLÍTICA DE ADMINISTRACIÓN

### 1.5.1 Especificación de la Organización Administradora

<b>Nombre</b>	Dirección Técnica de EDICOM
<b>Dirección de email</b>	<a href="mailto:acedicom@edicomgroup.com">acedicom@edicomgroup.com</a>
<b>Dirección</b>	Ronda de Auguste y Louis Lumière, 12 - Parque Tecnológico 46980 Paterna (Valencia) ESPAÑA
<b>Número de teléfono</b>	+34 902 119 229
<b>Número de fax</b>	+34 96 348 16 88

### 1.5.2 Persona de Contacto

<b>Nombre</b>	Departamento de sistemas de EDICOM
<b>Dirección de email</b>	<a href="mailto:acedicom@edicomgroup.com">acedicom@edicomgroup.com</a>
<b>Dirección</b>	Ronda de Auguste y Louis Lumière, 12 - Parque Tecnológico 46980 Paterna (Valencia) ESPAÑA
<b>Número de teléfono</b>	+34 902 119 229
<b>Número de fax</b>	+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 INFORMACIONES 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 detallan los procedimientos que se seguirán para acreditar la identidad del sujeto del certificado en el momento de registro y durante el ciclo de vida del certificado.

### 3.1 REGISTRO DE NOMBRES

#### 3.1.1 Tipos de nombres

Las extensiones *Subject Distinguished Name*, *Subject Alternative Names* o *Subject Directory Attributes* contienen información relativa al sujeto del certificado y es la que se usa para identificarlo.

La extensión *Subject Distinguished Name* ha de estar siempre presente. Su contenido dependerá del tipo de sujeto al que se emite el certificado:

- **Certificados de cliente TLS / email**
  - *CN (commonName)*: Contendrá el nombre y apellidos del titular del certificado, cuando estos datos hayan sido convenientemente acreditados y verificados. En caso de no necesitar incluir esta información o no poder verificarla correctamente, el contenido de este campo será "*ACEDICOM email certificate*".
  - *Email*: La dirección e-mail del titular del certificado. **Deberá** ser verificada en todo caso.
- **Certificados de servidor TLS**
  - *CN (commonName)*: Nombre DNS asignado al servidor para el que se emite. **Deberá** verificarse que el solicitante es el propietario o está debidamente autorizado por el propietario del dominio de nombres de Internet al que pertenece el servidor.
- **Certificados para firma de código**
  - *CN (commonName)*: Contendrá el nombre y apellidos del titular del certificado o de la empresa que lo solicita, cuando estos datos hayan sido convenientemente acreditados y verificados

Las comprobaciones de cualquier atributo a incluir en estos certificados serán llevadas a cabo tal y como especifica el punto 3.2 de las Prácticas de Certificación de ACEDICOM.

- **Firma de documentos:**

Firma con certificado no reconocido de documentos al sólo efecto de trazabilidad de flujos de trabajo e integridad de datos en aplicaciones internas. No requiere de validación presencial de la identidad de la persona y podrán ser solicitados individualmente o en grupos por un representante del proyecto o empresa donde se van a utilizar. En el campo Common Name (CN) figurarán los datos que permitan identificar más adecuadamente el sujeto firmante (personal, departamento, aplicación) dentro del flujo de trabajo. El campo email será opcional en estos certificados. A efectos de documentación se guardará el contrato de prestación de servicios de certificación y los documentos asociados al representante del proyecto o

empresa que firmará dicho contrato.

Podrán incluirse de forma opcional otros valores dentro de las extensiones mencionadas en este apartado siempre y cuando sean verificadas oportunamente.

Adicionalmente, se podrán incluir los siguientes campos dentro de *Subject Alternative Names* ya que habrán sido verificados obligatoriamente en todo caso:

- En caso de **certificados de cliente TLS / email**, el campo *RFC822 Name* para indicar la dirección de correo electrónico.
- En caso de **certificados de servidor TLS**, el campo *DNS Name* contiene la información del nombre DNS.

### 3.1.2 Significado de los nombres

Según RFC 3280 <http://www.ietf.org/rfc/rfc3280.txt>.

### 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

Dos Subject DN iguales sólo pueden coexistir si pertenecen al mismo suscriptor.

### 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.

### 3.1.7 Uso de comodines en los nombres

Los llamados comodines o *wildcards* en los nombres no están permitidos. Así pues, aunque es de uso común y se admite en Internet un certificado cuyo *CN* pueda ser, por ejemplo *CN=\*.dominio.tld*, al contener un comodín no podrá ser emitido al amparo de esta política.

Existe una única excepción: los certificados que se emitan para dominios bajo control de la organización administradora de ACEDICOM (ver 1.5.1 ) sí podrán contener comodines ya que la ACEDICOM tiene control en todo momento de los dominios y subdominios de los que la organización administradora es propietaria.

## 3.2 VERIFICACIÓN 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 o hardware.

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.

Esta política no contiene directrices sobre el tipo de dispositivo sobre el que se generan y almacenan las claves ya que es responsabilidad del solicitante.

### 3.2.2 Acreditación de identidad

Es requisito para el registro del certificado sea cual sea el tipo acreditar la identidad del sujeto del certificado que se desea registrar. En concreto, los datos que aparezcan en las extensiones que identifican al sujeto, mencionadas en el apartado 3.1.1, deberán ser verificados o de lo contrario su inclusión no será posible.

La verificación inicial de la identidad para los datos de obligada inclusión en el certificado depende del sujeto del mismo y es como sigue:

- **Certificados de cliente TLS / email:** se verificará la dirección de correo electrónica del solicitante, de forma que una vez iniciado el proceso de solicitud de certificado, se le darán las instrucciones necesarias para continuar con el mismo a través de la dirección electrónica especificada en la solicitud y destinada a ser incluida en el certificado.
- **Certificados de servidor TLS:** se verificará que la persona o entidad solicitante controlan el dominio de internet indicado en el *CN*. Una vez iniciado el proceso de solicitud de certificado, se le darán las instrucciones necesarias para continuar con el mismo a través de la vía de contacto (correo electrónico, teléfono o dirección física) especificada en la solicitud y que **deberá coincidir** con el contacto administrativo listado en el whois del dominio.
- **Certificados de firma de código:** Se verificará cualquier atributo a incluir en el certificado.
- **Firma de documentos:**
  - No requiere de validación presencial de la identidad de la persona y podrán ser solicitados individualmente o en grupos por un representante del proyecto o empresa donde se van a utilizar. En el campo Common Name (CN) figurarán los datos que permitan identificar más adecuadamente el sujeto firmante (personal, departamento, aplicación) dentro del flujo de trabajo. El campo email será opcional en estos certificados. A efectos de documentación se guardará el contrato de prestación de servicios de certificación y los documentos asociados al representante del proyecto o empresa que firmará dicho contrato.

En los procesos de comprobación de la propiedad de una dirección de correo electrónico, ACEIDCOM incluirá en el e-mail una cadena aleatoria e irreplicable, que conformará un desafío. El receptor del correo electrónico responderá al desafío siguiendo las instrucciones indicadas en el propio correo. Dicho desafío es asociado de forma inequívoca con la solicitud de emisión de certificado. Cuando el operador de registro compruebe que la respuesta al desafío es correcta, quedará demostrada la propiedad de la dirección de correo electrónico, y podrá continuar con el proceso de validación y emisión del certificado.

Dichos procesos de validación de control o propiedad de la dirección de correo electrónico son obligatorios en cada petición de emisión de certificados o renovación.

Cualquier otro dato adicional a incluir en el certificado deberá ser pertinentemente verificado. En todo caso ACEDICOM se reserva el derecho para requerir presencia física del solicitante o persona autorizada por el mismo en los Puntos de registro autorizados con el objeto de aportar documentación y realizar las verificaciones de identidad oportunas, tal y como se detalla en la Declaración de Prácticas de Certificación en los puntos 3.2.2 y 3.2.3.

### **3.2.2.1 Certificados de uso interno de ACEDICOM**

Los certificados emitidos al personal de ACEDICOM y la organización administradora, así como los emitidos para la infraestructura relacionada (servidores, email, etc) no requerirán guardar la documentación asociada a la validación de identidad.

## **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**

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 la sección 3.2.2. de forma que se garantice de manera fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud.

## **3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE**

El suscriptor del certificado podrá solicitar la revocación del mismo acreditando su identidad mediante:

- Enviando un documento o e-mail firmado con el mismo certificado que desea revocar.
- Uso de los mecanismos descritos en el apartado 3.2.2.

No obstante, 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. Serán causas de revocación del certificado la pérdida de control por parte del suscriptor de:

- La dirección electrónica incluida en el caso de **certificados de cliente TLS / Email**.
- El dominio asociado al CN del certificado en el caso de **certificados de servidor TLS**.

## 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 como se describe en el punto 3.2.2 del presente documento y remitir vía fax, correo electrónico o personalmente 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 punto 3.2.2.

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

En el caso de certificados para **Firma de documentos** no se requiere de validación presencial de la identidad de la persona y podrán ser solicitados individualmente o en grupos por un representante del proyecto o empresa donde se van a utilizar. A efectos de documentación se guardará el contrato de prestación de servicios de certificación y los documentos asociados al representante del proyecto o empresa que firmará dicho contrato.

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 de uso general útiles para autenticación electrónica, firma, cifrado de información y seguridad de las comunicaciones.

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece este documento y de acuerdo con lo establecido en las extensiones 'Key Usage' y 'Extended Key Usage' del certificado, de acuerdo con lo especificado en la RFC 3280 <http://www.ietf.org/rfc/rfc3280.txt>.

## **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 Otras formas de divulgación de información de revocación disponibles**

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

#### **4.9.12 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 o hardware que está en poder exclusivo del propio suscriptor.

Es responsabilidad del suscriptor proteger con el debido celo la clave privada del certificado para que no escape a su control exclusivo.

# 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 adecuadamente.

#### 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 o hardware 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*".

<b>Signature algorithm parameters</b>	RSA MinModLen=2040
<b>Key generation algorithm</b>	rsagen1
<b>Cryptographic padding method</b>	emsa-pkcs1-v1_5
<b>Hash function</b>	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 o hardware 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.

### 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 CERTIFICADOS 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

No aplicable.

### 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 debidamente.

### **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.

### **6.2.6 Método de activación de la clave privada**

No aplicable.

### **6.2.7 Método de desactivación de la clave privada**

No aplicable.

### **6.2.8 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 dos (2) 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 dos (2) 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.
- *ExtendedKeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *Subject Directory Attributes*. Calificada como no crítica.
- *Subject Alternative Names*. Calificada como no crítica
- *CRLDistributionPoints*. Calificada como no crítica.
- *Authority Information Access*. Calificada como no crítica.
- *TimeStamping*. Calificada como no crítica

El perfil de los certificados emitidos bajo esta política son:

Versión					
<b>Versión</b>	v3	S	A		F
<b>Serial Number</b>	Asignado automáticamente por la AC	S	A		F
<b>Signature Algorithm</b>	SHA1withRSAEncryption	S	A		F
<b>Issuer Distinguished Name</b>	Emite ACEDICOM Servidores: CN=ACEDICOM Servidores, OU=PKI, O=EDICOM, C=ES Emite ACEDICOM 01: CN=ACEDICOM 01, OU=PKI, O=EDICOM, C=ES Emite ACEDICOM 02: CN=ACEDICOM 02, OU=PKI, O=EDICOM, C=ES	S	A		F
<b>Validez</b>	2 años	S	A		F
<b>Subject Public Key Info</b>	Tipo de clave: RSA Longitud de la clave: 2048 bits	S	A		F
<b>Subject DN</b>		S	A		D
CommonName (CN)	ACEDICOM email certificate / Apellidos, Nombre servidor.dominio (autenticación de servidor)	S	C		F / D
CommonName (CN)	Nombre del titular o empresa (resto de casos)	S	S		D
Organización (O)	Nombre de la empresa	C	C		D
Departamento (OU)	Departamento dentro de la empresa	C	C		D
País (C)	País	C	C		D
Email	buzon@dominio	C	C		
<b>Subject Alternative</b>			A		

<b>Names</b>					
E-Mail (RFC 822)	Dirección de E-Mail del sujeto	O	C		D
DNS Name	Servidor.dominio	O	S		
MS UPN	Usuario@dominio (Active Directory)	O	C		D
<b>SubjectKeyIdentifier</b>	Identificador de la clave pública del certificado	S	A		D
<b>AuthorityKeyIdentifier</b>	Identificador de la clave pública asociada a la clave privada de la CA usada para firmar el presente certificado	S	A		F
<b>BasicConstraints</b>		S	A	X	F
CA	Falso	S	A	X	F
pathLength	No aplicable (0)		A		F
<b>KeyUsage</b>	DigitalSignature KeyEncipherment DataEncipherment KeyAgreement	S	A	X	F
<b>Certificate Policies</b>		S	A		F
policyIdentifier	1.3.6.1.4.1.30051.2.1.2.6.1	S	A		F
CPSuri	<a href="http://acedicom.edicomgroup.com">http://acedicom.edicomgroup.com</a>	S	A		F
policyIdentifier	1.3.6.1.4.1.30051.2.1.2.6.1	S	A		F
userNotice	Certificate Policy for TLS Client or Server	S	A		F
<b>ExtendedKeyUsage</b>		S	A	X	F
Client Authentication	- presente -	S	C		F
Client Authentication	- opcional -	O	S		
Email Protection	- presente -	S	C		
Server Authentication	- presente -	S	S		
MS Smart Card Logon	- opcional -	O	C		
Internet Key Exchange for IPSEC	- opcional -	O	A		
Code signing	- opcional -	O	CS		
	-opcional-	O	S	X	F
<b>CRLDistributionPoints</b>		S	A		F
distributionPoint	Emite ACEDICOM Servidores <a href="http://acedicom.edicomgroup.com/servidoresca.crl">http://acedicom.edicomgroup.com/servidoresca.crl</a> Emite ACEDICOM 01 <a href="http://acedicom.edicomgroup.com/acedicom01.crl">http://acedicom.edicomgroup.com/acedicom01.crl</a> Emite ACEDICOM 02 <a href="http://acedicom.edicomgroup.com/acedicom02.crl">http://acedicom.edicomgroup.com/acedicom02.crl</a>	S	A		F
<b>Authority Information Access</b>		S	A		F
accessMethod	CaIssuers (indicamos la información de revocación de la CA que emitió el certificado de la CA emisora del presente certificado)	S	A		F
AccessLocation	<a href="http://www.edicomgroup.com/acedicom/certs/rootca.cer">http://www.edicomgroup.com/acedicom/certs/rootca.cer</a>	S	A		F
accessMethod	OCSP	S	A		F
AccessLocation	Emite ACEDICOM Servidores <a href="http://ocsp.acedicom.edicomgroup.com/servidores">http://ocsp.acedicom.edicomgroup.com/servidores</a> Emite ACEDICOM 01 <a href="http://ocsp.acedicom.edicomgroup.com/acedicom01">http://ocsp.acedicom.edicomgroup.com/acedicom01</a> Emite ACEDICOM 02 <a href="http://ocsp.acedicom.edicomgroup.com/acedicom02">http://ocsp.acedicom.edicomgroup.com/acedicom02</a>	S	A		F

Leyenda de la tabla:

- **I** = Incluida. Posibles valores: **S**=Siempre, **O**=Opcionalmente, **C**=Condicionalmente
- **Sujeto**. Posibles valores: **C**=Cliente TLS, **S**=Servidor TLS, **CS**=Firma de código, **A**=Ambos.
- **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.

### 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: 1.3.6.1.4.1.30051.2.1.2.6.1

## **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.

## **7.2 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.

# Anexo I: Solicitud de revocación

Intercambio Electrónico de Datos y Comunicaciones, S.L.  
Ronda de Auguste y Louis Lumiere, 12 \_ 46980 Parque Tecnológico (Valencia) Spain  
Phone 902 11 92 28 Fax: +34 961 36 71 17 www.edicomgroup.com



## SOLICITUD DE REVOCACION DE CERTIFICADO

### DATOS IDENTIFICATIVOS DE LA PERSONA FISICA SOLICITANTE

NIF : \_\_\_\_\_ APELLIDOS Y NOMBRE : \_\_\_\_\_

DOMICILIO: \_\_\_\_\_ CODIGO POSTAL: \_\_\_\_\_

POBLACION : \_\_\_\_\_ PROVINCIA/PAÍS : \_\_\_\_\_

### DATOS DE CONTACTO

TELEFONO : \_\_\_\_\_ FAX : \_\_\_\_\_ E-MAIL : \_\_\_\_\_

### DATOS DE REPRESENTACION (Marque X según proceda)

REPRESENTACIÓN ORGANICA (Representante Legal/Administrador)  REPRESENTACION VOLUNTARIA (Poder especial y expreso)

### DATOS DE LA PERSONA JURIDICA TITULAR DEL CERTIFICADO

NIF : \_\_\_\_\_ RAZON SOCIAL: \_\_\_\_\_

DOMICILIO: \_\_\_\_\_ CODIGO POSTAL: \_\_\_\_\_

POBLACION : \_\_\_\_\_ PROVINCIA/PAÍS : \_\_\_\_\_

TIPO DE CERTIFICADO : \_\_\_\_\_

NUMERO DE SERIE DEL CERTIFICADO: \_\_\_\_\_

MOTIVO DE LA REVOCACION: (La simple voluntad de revocación del suscriptor del certificado es un motivo válido para la solicitud de la misma) :

\_\_\_\_\_  
\_\_\_\_\_

El solicitante :  
Fecha: