COLEGIO DE REGISTRADORES DE LA PROPIEDAD Y MERCANTILES DE ESPAÑA

Prestador del Servicio de Certificación de Registradores

Política de Certificación de los Certificados Internos

Versión 1.0.9

03 de Marzo de 2015

Firmado digitalmente por NOMBRE GALLEGO FERNANDEZ LUIS ANTONIO - NIF 34979668A
Nombre de reconocimiento (DN): c=ES, o=Colegio de Registradores de la Propiedad y Mercantiles de España, ou=UNIDAD TRAMITACION CENTRAL, cn=NOMBRE GALLEGO FERNANDEZ LUIS ANTONIO - NIF 34979668A
Fecha: 2015.03.11 09:48:22 +01'00'

CONTROL DOCUMENTAL

DOCUMENTO/ARCHIVO	
Título: **Política de Certificación de Certificados Internos**	Nombre Archivo/s:
Código:	Soporte lógico:
Fecha: **03/03/2015**	Ubicación física:
Versión: **Versión 1.0.9**	

REGISTRO DE CAMBIOS		
Versión	Fecha	Motivo del cambio
1.0	19/01/2007	Versión inicial
1.0.5	30/12/2008	Adaptación Requerimiento Industria
1.0.6	29/04/2009	Corrección OIDs de los certificados
1.0.7	26/10/2011	Adaptación Requerimiento Industria
1.0.8	01/07/2014	Actualización de los datos del PSC Incorporación de información relacionada al ciclo de vida de los certificados no reconocidos SSL
1.0.9	03/03/2015	Actualización de los perfiles de certificación 4. Auth. Information – OCPS a protocolo HTTP

DISTRIBUCIÓN DEL DOCUMENTO	
Nombre	Área

CONTROL DEL DOCUMENTO			
PREPARADO	**REVISADO**	**APROBADO**	**ACEPTADO**
José Antonio Romero	Arjan Sundardas Mirchandani	Joaquín Rodríguez Hernández	
Comité Técnico de Asesoramiento y Cumplimiento Normativo	Director Técnico del Servicio de Sistemas de Información	Comisión Directora	**Junta de Gobierno**

Índice

1. INTRODUCCIÓN 10

1.1. Visión general 10

1.2. Nombre del documento e identificación de la PC 10

1.3. Participantes en la infraestructura de clave pública (PKI) del prestador del Servicio de Certificación del Colegio de Registradores 11

1.3.1. Prestador de Servicios de Certificación (PSC) 11

1.3.2. Autoridad de Aprobación de Políticas 12

1.3.3. Autoridad de Certificación Raíz 12

1.3.4. Autoridades de Certificación Subordinadas 13

1.3.5. Autoridad de Registro 14

1.3.6. Autoridad de Validación (VA) 14

1.3.7. Autoridad de Sellado de Tiempo (TSA) 15

1.3.8. Entidades finales 15

1.4. Uso de los certificados 16

1.4.1. Usos adecuados de los certificados 16

1.4.2. Limitaciones y restricciones en el uso de los certificados 16

1.5. Administración de las políticas 16

1.5.1. Entidad Responsable 16

1.5.2. Procedimiento de aprobación y modificación de la Declaración de Prácticas de Certificación 17

1.6. Datos de Contacto 17

1.7. Definiciones y Acrónimos 17

1.7.1. Definiciones 17

1.7.2. Acrónimos 20

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN 22

Directorio de Validación de Certificados 22

2.1. 22

2.2. Publicación de información de certificación 22

2.3. Frecuencia de publicación 23

2.4. Controles de acceso a la información de certificación 23

3. IDENTIFICACIÓN Y AUTENTICACIÓN 24

3.1. Nombres 24

3.1.1. Tipos de nombres 24

3.1.2. Necesidad de que los nombres sean significativos 25

3.1.3. Reglas para interpretar varios formatos de nombres 25

3.1.4. Unicidad de los nombres 25

3.1.5. Procedimientos de resolución de conflictos sobre nombres 26

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas 26

3.2. Validación inicial de la identidad 26

3.2.1. Medio de prueba de posesión de la clave privada 26
3.2.2. Autenticación de la identidad de una persona jurídica 26
3.2.3. Autenticación de la identidad de una persona física 26
3.2.4. Autenticación de la identidad de un dispositivo 27
3.2.5. Información no verificada sobre el solicitante 27
3.2.6. Comprobación de las facultades de representación 27
3.2.7. Criterios para operar con CA externas 27
3.3. Identificación y autenticación para solicitudes de renovación 27
3.4. Identificación y autenticación para solicitudes de revocación 28

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 29
4.1. Solicitud de certificados 29
4.1.1. Quién puede efectuar una solicitud 29
4.1.2. Registro de las solicitudes de certificados y responsabilidades de los solicitantes 31
4.2. Tramitación de las solicitudes de certificados 31
4.2.1. Realización de las funciones de identificación y autenticación 31
4.2.2. Aprobación o denegación de las solicitudes de certificados 31
4.2.3. Plazo para la tramitación de las solicitudes de certificados 31
4.3. Emisión de certificados 31
4.3.1. Actuaciones de la CA durante la emisión del certificado 31
4.3.2. Notificación al solicitante de la emisión por la CA del certificado 31
4.3.3. Licencia de Uso 32
4.4. Aceptación del certificado 33
4.4.1. Mecanismo de aceptación del certificado 33
4.4.2. Publicación del certificado por la CA 33
4.4.3. Notificación de la emisión del certificado por la CA a otras Autoridades 33
4.5. Par de claves y uso del certificado 33
4.5.1. Uso de la clave privada y del certificado por el titular 33
4.5.2. Uso de la clave pública y del certificado por los terceros aceptantes 33
4.6. Renovación de certificados sin cambio de claves 33
4.6.1. Circunstancias para la renovación de certificados sin cambio de claves 33
4.6.2. Quién puede solicitar la renovación de los certificados sin cambio de claves 33
4.6.3. Tramitación de las peticiones de renovación de certificados sin cambio de claves 33
4.6.4. Notificación de la emisión de un nuevo certificado al titular 33
4.6.5. Forma de aceptación del certificado sin cambio de claves 33
4.6.6. Publicación del certificado sin cambio de claves por la CA 34
4.6.7. Notificación de la emisión del certificado por la CA a otras Autoridades 34
4.7. Renovación de certificados con cambio de claves 34
4.7.1. Circunstancias para una renovación con cambio claves de un certificado 34
4.7.2. Quién puede pedir la renovación de los certificados 34
4.7.3. Tramitación de las peticiones de renovación de certificados con cambio de claves 34
4.7.4. Notificación de la emisión de un nuevo certificado al titular 34
Forma de 34
4.7.5. aceptación del certificado con las claves cambiadas 34
4.7.6. Publicación del certificado con las nuevas claves por la CA 35

4.7.7. Notificación de la emisión del certificado por la CA a otras Autoridades 35

4.8. Modificación de certificados 35
4.8.1. Circunstancias para la modificación de un certificado 35
4.8.2. Quién puede solicitar la modificación de los certificados 35
4.8.3. Tramitación de las peticiones de modificación de certificados 35
4.8.4. Notificación de la emisión de un certificado modificado al titular 35
4.8.5. Forma de aceptación del certificado modificado 35
4.8.6. Publicación del certificado modificado por la CA 35
4.8.7. Notificación de la modificación del certificado por la CA a otras Autoridades 35

4.9. Revocación y suspensión de certificados 35
4.9.1. Circunstancias para la revocación 35
4.9.2. Quién puede solicitar la revocación 36
4.9.3. Procedimiento de solicitud de revocación 36
4.9.4. Periodo de gracia de la solicitud de revocación 36
4.9.5. Plazo en el que la CA debe resolver la solicitud de revocación 36
4.9.6. Requisitos de verificación de las revocaciones por los terceros que confían 36
4.9.7. Frecuencia de emisión de CRL 36
4.9.8. Tiempo máximo entre la generación y la publicación de las CRL 36
4.9.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados 36
4.9.10. Requisitos de comprobación en línea de revocación 36
4.9.11. Otras formas de divulgación de información de revocación disponibles 36
4.9.12. Requisitos especiales de revocación de claves comprometidas 37
4.9.13. Causas para la suspensión 37
4.9.14. Quién puede solicitar la suspensión 37
4.9.15. Procedimiento para la solicitud de suspensión 37
4.9.16. Límites del periodo de suspensión 37

4.10. Servicios de información del estado de certificados 37
4.10.1. Características operativas 37
4.10.2. Disponibilidad del servicio 37
4.10.3. Características adicionales 37

4.11. Extinción de la validez de un certificado 37

4.12. Custodia y recuperación de claves 37
4.12.1. Prácticas y políticas de custodia y recuperación de claves 37
4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión 37

5. CONTROLES DE SEGURIDAD 38

5.1. Seguridad física 38
5.1.1. Ubicación y medidas de seguridad física de las instalaciones de CORPME 38
5.1.2. Acceso físico 38
5.1.3. Suministro eléctrico y acondicionamiento ambiental de las instalaciones del CORPME 38
5.1.4. Exposición al agua 38
5.1.5. Medidas contra incendios e inundaciones. 38
5.1.6. Sistema de almacenamiento 38
5.1.7. Eliminación de residuos 38
5.1.8. Política de Respaldo de Información. 38

5.2. Controles de procedimiento 38
5.2.1. Roles responsables del control y gestión de la PKI del CORPME 38
5.2.2. Número de personas requeridas por tarea 38
5.2.3. Roles que requieren segregación de funciones 39
5.3. Controles de personal 39
5.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales 39
5.3.2. Procedimientos de comprobación de antecedentes 39
5.3.3. Requerimientos de formación 39
5.3.4. Requerimientos y frecuencia de actualización de la formación 39
5.3.5. Frecuencia y secuencia de rotación de tareas 39
5.3.6. Sanciones por actuaciones no autorizadas 39
5.3.7. Requisitos de contratación de terceros 39
5.3.8. Documentación proporcionada al personal 39
5.4. Procedimientos de auditoría de seguridad 39
5.4.1. Tipos de eventos registrados 39
5.4.2. Frecuencia de procesado de registros de auditoría 39
5.4.3. Periodo de conservación de los registros de auditoría 39
5.4.4. Protección de los registros de auditoría 40
5.4.5. Procedimientos de respaldo de los registros de auditoría 40
5.4.6. Sistema de recogida de información de auditoría (interno vs externo) 40
5.4.7. Notificación al sujeto causa del evento 40
5.4.8. Análisis de vulnerabilidades 40
5.5. Archivado de registros 40
5.5.1. Tipo de eventos archivados 40
5.5.2. Periodo de conservación de registros 40
5.5.3. Protección del archivo 40
5.5.4. Procedimientos de copia de respaldo del archivo 40
5.5.5. Requerimientos para el sellado de tiempo de los registros 40
5.5.6. Sistema de archivo de información de auditoría (interno vs externo) 40
5.5.7. Procedimientos para obtener y verificar información archivada 40
5.6. Cambio de claves 40
5.7. Recuperación ante compromiso de clave o catástrofe 41
5.7.1. Procedimientos de gestión de incidentes y compromisos 41
5.7.2. Alteración de los recursos hardware, software y/o datos 41
5.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad 41
5.7.4. Instalación después de un desastre natural u otro tipo de catástrofe 41
5.8. Cese de una CA o RA 41
5.8.1. Autoridad de Certificación 41
5.8.2. Autoridad de Registro 41

6. CONTROLES DE SEGURIDAD TÉCNICA 42
6.1. Generación e instalación del par de claves 42
6.1.1. Generación del par de claves 42
6.1.2. Entrega de la clave privada al titular 42
6.1.3. Entrega de la clave pública al emisor del certificado 42

6.1.4. Entrega de la clave pública de la CA a los terceros que confían ... 42
6.1.5. Tamaño de las claves ... 42
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad ... 42
6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509 v3) ... 42
6.2. Protección de la clave privada y controles de ingeniería de los módulos ... 42
6.2.1. Estándares para los módulos criptográficos ... 42
6.2.2. Control multipersona (k de n) de la clave privada ... 43
6.2.3. Custodia de la clave privada ... 43
6.2.4. Copia de seguridad de la clave privada ... 43
6.2.5. Archivo de la clave privada ... 43
6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico ... 43
6.2.7. Almacenamiento de la clave privada en un módulo criptográfico ... 43
6.2.8. Método de activación de la clave privada ... 43
6.2.9. Método de desactivación de la clave privada ... 43
6.2.10. Método de destrucción de la clave privada ... 43
6.2.11. Clasificación de los módulos criptográficos ... 43
6.3. Otros aspectos de la gestión del par de claves ... 43
6.3.1. Archivo de la clave pública ... 43
6.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves ... 43
6.4. Datos de activación ... 44
6.4.1. Generación e instalación de los datos de activación ... 44
6.4.2. Protección de los datos de activación ... 44
6.4.3. Otros aspectos de los datos de activación ... 44
6.5. Controles de seguridad informática ... 44
6.5.1. Requerimientos técnicos de seguridad específicos ... 44
6.5.2. Evaluación de la seguridad informática ... 44
6.6. Controles de seguridad del ciclo de vida ... 44
6.6.1. Controles de desarrollo de sistemas ... 44
6.6.2. Controles de gestión de seguridad ... 44
6.6.3. Controles de seguridad del ciclo de vida ... 44
6.7. Controles de seguridad de la red ... 44
6.8. Sellado de tiempo ... 44

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP ... 45
7.1. Perfil de certificado ... 45
7.1.1. Número de versión ... 45
7.1.2. Extensiones del certificado ... 45
7.1.3. Identificadores de objeto (OID) de los algoritmos ... 48
7.1.4. Formatos de nombres ... 48
7.1.5. Restricciones de los nombres ... 48
7.1.6. Identificador de objeto (OID) de la Política de Certificación ... 48
7.1.7. Uso de la extensión "PolicyConstraints" ... 48
7.1.8. Sintaxis y semántica de los "PolicyQualifier" ... 48
7.1.9. Tratamiento semántico para la extensión crítica "Certificate Policy" ... 48
7.2. Perfil de CRL ... 49

7.2.1. Número de versión 49
7.2.2. CRL y extensiones 49
7.3. Perfil de OCSP 49
7.3.1. Número(s) de versión 49
7.3.2. Extensiones OCSP 49

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES 50
8.1. Frecuencia o circunstancias de los controles para cada Autoridad 50
8.2. Identificación/cualificación del auditor 50
8.3. Relación entre el auditor y la Autoridad auditada 50
8.4. Aspectos cubiertos por los controles 50
8.5. Acciones a tomar como resultado de la detección de deficiencias 50
8.6. Comunicación de resultados 50

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD 51
9.1. Tarifas 51
9.1.1. Tarifas de emisión o renovación de certificado 51
9.1.2. Tarifas de acceso a los certificados 51
9.1.3. Tarifas de acceso a la información de estado o revocación 51
9.1.4. Tarifas de otros servicios tales como información de políticas 51
9.1.5. Política de reembolso 51
9.2. Responsabilidades económicas 51
9.3. Confidencialidad de la información 51
9.3.1. Ámbito de la información confidencial 51
9.3.2. Información no confidencial 51
9.3.3. Deber de secreto profesional 51
9.4. Protección de la información personal 51
9.5. Derechos de propiedad intelectual 52
9.6. Representaciones y garantías 52
9.6.1. Obligaciones de las CA 52
9.6.2. Obligaciones de las RA 52
9.6.3. Obligaciones de los titulares de los certificados 52
9.6.4. Obligaciones de los terceros que confían o aceptan los certificados del CORPME 52
9.6.5. Obligaciones de otros participantes 52
9.7. Exención de responsabilidades 52
9.8. Limitaciones de las responsabilidades 52
9.9. Indemnizaciones 52
9.10. Período de validez 52
9.10.1. Plazo 52
9.10.2. Sustitución y derogación de la PC 52
9.10.3. Efectos de la finalización 53
9.11. Notificaciones individuales y comunicaciones con los participantes 53

9.12. Procedimientos de cambios en las especificaciones 53
9.12.1. Procedimiento para los cambios 53
9.12.2. Circunstancias en las que el OID debe ser cambiado 53
9.13. Reclamaciones 53
9.14. Normativa aplicable 53
9.15. Cumplimiento de la normativa aplicable 53
9.16. Estipulaciones diversas 53
9.16.1. Cláusula de aceptación completa 53
9.16.2. Independencia 53
9.16.3. Resolución por la vía judicial 54
9.17. Otras estipulaciones 54

1. INTRODUCCIÓN

1.1. VISIÓN GENERAL

El Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España (en adelante CORPME), Corporación de Derecho Público adscrita a la Dirección General de los Registros y el Notariado del Ministerio de Justicia, se constituye como Prestador de Servicios de Certificación de Firma Electrónica en virtud del mandato efectuado por el Legislador en la disposición adicional 26ª de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. Nace con la finalidad de ofrecer los mecanismos y sistemas necesarios para garantizar la seguridad de las comunicaciones telemáticas en las que intervengan los Registradores, las Administraciones Publicas, los profesionales que se relacionan con los Registros y los ciudadanos en general.

El Reglamento interno del PSC del CORPME es la norma básica del Servicio de Certificación, en la que se establecen su naturaleza, estructura y organización, así como los criterios y procedimientos que el Servicio se compromete a seguir en el ejercicio de su actividad, incluyendo desde la solicitud de los certificados y generación de las claves, hasta la posterior emisión, distribución, uso, revocación y renovación de los mismos.

La Declaración de Prácticas de Certificación (en adelante DPC), emitida de conformidad con el Art.19 de la Ley 59/2003, de Firma Electrónica, así como con la RFC3647, define y documenta un marco normativo general, conforme al cual se desarrollará la actividad de Prestador del Servicio de Certificación del CORPME, en relación con los procesos de solicitud, emisión y gestión del ciclo de vida de los certificados digitales, incluyendo los procedimientos de verificación de la vigencia, revocación y renovación de certificados.

Las Políticas de Certificación (en adelante PC's) aplicables a cada clase de certificado complementan lo dispuesto con carácter general en la DPC. En caso de conflicto o contradicción entre lo dispuesto en la Declaración de Prácticas de Certificación y las citadas Políticas, prevalecerá lo preceptuado en estas últimas.

Las PC's también definen el ámbito de potenciales titulares de los certificados, así como los usos previstos de los certificados emitidos por el CORPME.

La actividad del CORPME se desarrollará con plena sujeción a las prescripciones de la Ley 24/2001, de 27 de diciembre, la ley 59/2003 de Firma Electrónica, de 20 de diciembre, y al Reglamento interno del PSC.

Esta PC asume que el lector conoce los conceptos de PKI, certificado y Firma Electrónica; 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. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DE LA PC

El presente documento se denomina *POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS INTERNOS DEL CORPME.*

Identificación del Documento:

Nombre del documento	Políticas de Certificación de Certificados Internos del CORPME
Versión del documento	1.0.8

Estado del documento	Versión
Fecha de emisión	01/07/2014
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.1.0.1.0
Ubicación de la PC	http://pki.registradores.org/normativa/index.htm
DPC Relacionada	Declaración de Prácticas de Certificación del CORPME

1.3. PARTICIPANTES EN LA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) DEL PRESTADOR DEL SERVICIO DE CERTIFICACIÓN DEL COLEGIO DE REGISTRADORES

1.3.1. Prestador de Servicios de Certificación (PSC)

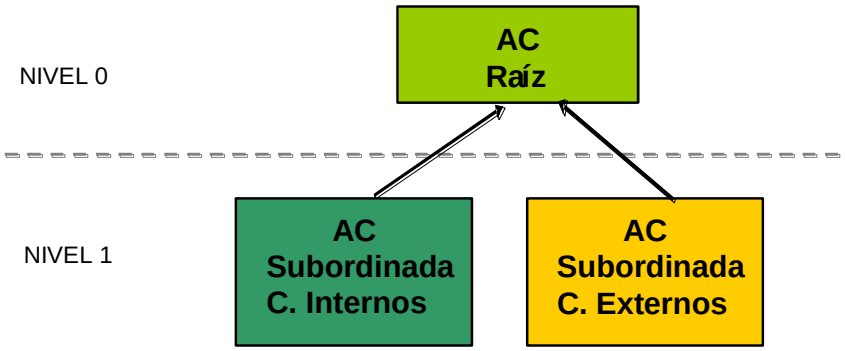
Es la entidad responsable de la emisión, bajo la jerarquía de su certificado raíz, de los certificados digitales destinados a entidades finales, así como de la gestión del ciclo de vida de los certificados digitales.

La información legal y datos identificativos del Prestador de Servicios de Certificación del CORPME estarán siempre disponibles en http://pki.registradores.org/normativa/index.htm. También podrá solicitarse una copia impresa de dicha documentación previa solicitud del interesado en la dirección siguiente:

Colegio de Registradores de la Propiedad, Mercantiles y de Bienes muebles de España.
Prestador del Servicio de Certificación del Colegio de Registradores
C/ DIEGO DE LEON, 21.
28006-MADRID

En el CORPME concurre además de la condición de prestador (PSC), la de CA (Certification Authority), desarrollando su actividad de conformidad con la legislación vigente en la materia, señaladamente la ley 59/2003, de 20 de diciembre de Firma Electrónica.

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



1.3.2. Autoridad de Aprobación de Políticas

La Autoridad de Aprobación de Políticas (en adelante AAP) es la organización responsable de la aprobación de la DPC y de las Políticas de Certificación del CORPME así como de la aprobación de las modificaciones de dichos documentos.

Asimismo, la AAP es la responsable, en caso de que se tuviese que evaluar la posibilidad de que una CA externa interactúe con la PKI del CORPME, de determinar la adecuación de la DPC de dicha CA a la Política de Certificación afectada.

La AAP es responsable de analizar los informes de las auditorías, ya sean estos totales o parciales que se hagan de la PKI, así como de determinar en caso necesario, las acciones correctoras a ejecutar.

La AAP estará formada por la Comisión Directora, órgano máximo directivo del CORPME constituida por los siguientes vocales:

- Vocal del Servicio de Coordinación de las Oficinas Liquidadoras del CORPME, que actúa como Presidente del Comité.
- Vocal Secretario del CORPME.
- Vocal del Servicio de Coordinación de Registros Mercantiles del CORPME.
- Vocal del Servicio de Sistemas de Información del CORPME.

1.3.3. Autoridad de Certificación Raíz

El CORPME emite todos los certificados objeto de la DPC bajo la jerarquía del Certificado de la clave principal, o certificado raíz. El certificado raíz es un certificado *auto-firmado*, con el que se inicia la cadena de confianza.

De manera subordinada a la Raíz, se encuentran los certificados de jerarquía o de clave secundaria, que serán uno para los Certificados Internos y otro para los Certificados Externos.

El titular del certificado Raíz es el propio CORPME, y se emite y revoca por la Unidad de Tramitación Central, a solicitud de la Comisión Directora, de conformidad con el procedimiento definido en el Reglamento interno del PSC.

La información más relevante de la Autoridad de Certificación Raíz del CORPME es la siguiente:

Nombre distintivo	CN = Registradores de España - CA Raíz, OU = Certificado Propio, O = Colegio de Registradores de la Propiedad y Mercantiles de España, C = ES
Número de serie	2d e4 0a e1 9b d1 c2 aa 4c f4 00 ac 81 35 f9
Nombre distintivo del emisor	CN = Registradores de España - CA Raíz, OU = Certificado Propio, O = Colegio de Registradores de la Propiedad y Mercantiles de España, C = ES
Fecha de emisión	09/01/2007
Fecha de expiración	09/01/2031
Longitud de clave RSA	4096 Bits
Huella digital (SHA-1)	21 11 65 ca 37 9f bb 5e d8 01 e3 1c 43 0a 62 aa c1 09 bc b4
URL de publicación del certificado	http://pki.registradores.org/certificados/ca_raiz_scr.crt

1.3.4. Autoridades de Certificación Subordinadas

Bajo la jerarquía de la clave principal o certificado Raíz del CORPME**,** se encuentran los certificados de la *Clave Secundaria para Certificados Internos* y de la *Clave Secundaria para Certificados Externos*, bajo cuyas respectivas jerarquías se emiten a su vez todos los certificados que el CORPME emite a entidades finales.

La información más relevante de la CA subordinada para **Certificados Internos** es la siguiente:

Nombre distintivo	CN = Registradores de España - CA Interna, OU = Certificado Propio, O = Colegio de Registradores de la Propiedad y Mercantiles de España, C = ES
Número de serie	38 ad a8 70 c7 1e 03 4f 45 c0 69 7a 1b eb ba b5
Nombre distintivo del emisor	CN = Registradores de España - CA Raíz, OU = Certificado Propio, O = Colegio de Registradores de la Propiedad y Mercantiles de España, C = ES
Fecha de emisión	31/01/2007
Fecha de expiración	31/01/2019
Longitud de clave RSA	2048 Bits
Huella digital (SHA-1)	26 73 e8 85 5f 11 d9 f3 1a c5 f9 13 65 0c 1d d7 44 8b d3 07
URL de publicación del certificado	http://pki.registradores.org/certificados/ca_int_scr.crt
URL de publicación de la CRL	http://pki.registradores.org/crls/crl_int_scr.crl
Tipos de certificados emitidos	Certificado Reconocido de Registrador Certificado Reconocido para Personal Interno Certificado no Reconocido para procedimientos registrales Certificado no Reconocido de servidor SSL

La información más relevante de la CA subordinada para **Certificados Externos** es la siguiente:

Nombre distintivo	CN = Registradores de España - CA Externa, OU = Certificado Propio, O = Colegio de Registradores de la Propiedad y Mercantiles de España, C = ES
Número de serie	7e fd af cb 1b eb c1 1b 45 c0 69 a3 02 a7 4b 46
Nombre distintivo del emisor	CN = Registradores de España - CA Raíz, OU = Certificado Propio, O = Colegio de Registradores de la Propiedad y Mercantiles de España, C = ES
Fecha de emisión	31/01/2007
Fecha de expiración	31/01/2019
Longitud de clave RSA	2048 Bits
Huella digital (SHA-1)	ca 2b 66 c7 cb 2a a1 e9 c7 29 80 29 3b b6 6a 48 56 36 8a 94

URL de publicación del certificado	http://pki.registradores.org/certificados/ca_ext_scr.crt
URL de publicación de la CRL	http://pki.registradores.org/crls/crl_ext_scr.crl
Tipos de certificados emitidos	Certificado Reconocido Personal Certificado Reconocido de Representante de Persona Jurídica Certificado Reconocido de Cargo Administrativo Certificado Reconocido de Administración Local Certificado Reconocido de Profesional

1.3.5. Autoridad de Registro

La Autoridad de Registro del PSC del CORPME, está formada por sus Unidades de Tramitación, y engloban a:

- Registros Mercantiles
- Decanatos
- Registros de la Propiedad
- Unidad de Tramitación Central

Éstas redactan el contenido de los certificados tras realizar las comprobaciones precisas y autorizan su emisión o revocación. Para los certificados personales, las Unidades de Tramitación generarán en un dispositivo seguro los pares de claves criptográficas para su entrega a los solicitantes.

Todas las Unidades de Tramitación estarán bajo la supervisión y dirección de un registrador titular, interno o accidental, salvo;

- Los Decanatos, cuyo responsable será el Decano territorial, o un registrador asignado por él.
- La Unidad de Tramitación Central, cuyo responsable será cualquier miembro de la Junta de Gobierno, designado por el vocal del Servicio de Sistemas de Información, (en adelante SSI).

La Unidad de Tramitación Central será la encargada de la emisión o revocación de los certificados de dispositivos (SSL), bajo solicitud aprobada según el procedimiento de gestión de solicitudes y validada esta solicitud por el Director Técnico del SSI del CORPME.

Todas las Autoridades de Registro funcionan bajo la supervisión y coordinación de la Comisión Directora y precisan de la previa habilitación de la Junta de Gobierno del CORPME, para la emisión de cada una de las clases de certificados.

La expedición de determinados certificados digitales del CORPME se verificará, previa petición de cita en línea del solicitante, en la dirección de Internet **https://www.registradores.org/scr/agenda**, en una única comparecencia, el día y hora de su elección en la Unidad de Tramitación.

1.3.6. Autoridad de Validación (VA)

La Autoridad de Validación (VA) tiene como función facilitar el estado de los certificados emitidos por el PSC del CORPME, mediante el protocolo Online Certificate Status Protocol (OCSP), que determina el estado actual de un certificado electrónico a solicitud de un tercero aceptante sin requerir el acceso a listas de certificados revocados por éstas.

Este mecanismo de validación es complementario a la publicación de las listas de certificados revocados (CRL).

1.3.7. Autoridad de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo (TSA) es la responsable de la prestación de los servicios recogidos a continuación, de forma que proporcione confianza a sus usuarios: solicitantes, suscriptores y terceros aceptantes.

Los servicios de sellado de tiempo se estructuran en dos partes:

- **Suministro de los sellos de tiempo**: los componentes técnicos y organizativos que emiten los sellos de tiempo (TST).
- **Gestión del sellado de tiempo**: los componentes técnicos y organizativos que supervisan y controlan la operativa del sellado de tiempo, incluyendo la sincronización temporal con la fuente de referencia UTC.

La TSA tiene la responsabilidad de operar una o varias Unidades de Sellado de Tiempo (TSU) las cuales crearán y firmarán los sellos de tiempo (TST) en nombre de la TSA. Las claves privadas de las TSA serán comunes y estarán compartidas entre ellas.

La TSA queda identificada en el certificado electrónico de firma que se utilice en el servicio de sellado de tiempo.

1.3.8. Entidades finales

Se definen como entidades finales aquellas personas físicas sujetos de derechos, con capacidad suficiente para solicitar y obtener un certificado digital del CORPME, a título propio o en su condición de representante de una persona jurídica. También se consideran entidades finales los Terceros de buena fe que confían en los certificados del CORPME.

A los efectos anteriores tendrán la consideración de Entidades Finales:

- Solicitante
- Suscriptor
- Tercero que confía en los certificados de CORPME.

1.3.8.1. Solicitante

Cuando un interesado en obtener un certificado emitido por el CORPME, cumplimenta el formulario de petición de cita de **https://www.registradores.org/scr/agenda**, adquiere la condición de Solicitante. La mera solicitud de un certificado no implica la concesión del mismo, la cual queda supeditada al éxito de procedimiento de Registro ante la Unidad de Tramitación correspondiente, previa verificación de la información correspondiente al certificado que el solicitante facilita.

Sólo las personas mayores de edad podrán solicitar y, en su caso, obtener certificados digitales del CORPME.

1.3.8.2. Suscriptor

Se denomina suscriptor, de conformidad con lo dispuesto en el artículo 6 de la Ley 59/2003, a la persona física cuya identidad se vincula a unos *Datos de creación y verificación de Firma*, a través de una C*lave Pública* certificada (firmada digitalmente) por el *Prestador de Servicios de Certificación*. Los datos de identificación del Suscriptor están contenidos en el campo "*Subject*" del certificado definido dentro del estándar X509 de la ITU.

En tanto que el CORPME únicamente expide certificados digitales a personas físicas y no jurídicas, en el caso de los Certificados de Representante de Persona Jurídica, tendrá la consideración de Suscriptor a los efectos de la Ley de Firma Electrónica, la persona física que en virtud de apoderamiento inscrito en el Registro Mercantil ostente la representación de una persona jurídica, incluyéndose los datos de ésta en el certificado.

La identidad del Suscriptor en tanto que titular del certificado figurara en el campo *Distinguished Name* del certificado digital en el campo *CN=Common Name*, dentro de la extensión *Subject* del

certificado. Los datos identificativos del Suscriptor podrán ser así mismo incluidos, dependiendo del tipo de certificado, con formato RFC6854 en una extensión de nombre alternativo *subjectAltName*, de conformidad con lo que se estipule en las políticas particulares aplicables a cada certificado.

1.3.8.3. Tercero que confía en los Certificados de CORPME

A los efectos de esta PC, Tercero es cualquier usuario que deposita su confianza en los certificados emitidos por el CORPME, y utilizados para la firma de comunicaciones, documentos electrónicos, o en la autenticación ante sistemas basada en certificados digitales.

El CORPME no asume ningún tipo de responsabilidad ante terceros, incluso de buena fe, que no hayan aplicado la diligencia debida para la verificación de la vigencia de los Certificados.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos adecuados de los certificados

Los certificados regulados por esta PC se utilizarán para:

- **Certificados de Autenticación y Firma**: Estos certificados se utilizarán para la autenticación de personas frente a los Sistemas de Información del CORPME así como para la generación de firmas electrónicas avanzadas.
- **Certificados de Componente:** El uso de estos certificados se establece para vincular unos datos de verificación de la firma, que podrá ser del servidor donde está instalado o de la aplicación correspondiente, a un suscriptor que tiene el control del funcionamiento del componente que utiliza el certificado.

1.4.2. Limitaciones y restricciones en el uso de los certificados

Cualquier uso no incluido en el apartado anterior queda excluido.

1.5. ADMINISTRACIÓN DE LAS POLÍTICAS

1.5.1. Entidad Responsable

El SSI a través de su Comité técnico de Asesoramiento y Cumplimiento Normativo, constituido por;

- El Director de Tecnología y Sistemas, que actúa como Presidente del Comité.
- El Director de la Oficina de Seguridad y Cumplimiento Normativo, que actuará como Secretario.
- El Director de Infraestructuras, Ingeniería de la Seguridad y Comunicaciones
- El Director de Tecnologías Wintel y Virtualización
- El Director de Operaciones
- Un Director de Proyectos y Servicios, en representación de los directores de Proyectos y Servicios

Establecerá los términos y redacción de la PC del CORPME. En aquellos casos en que de conformidad con lo dispuesto en el Reglamento interno del PSC sea preceptivo, la Comisión Directora actuará por mandato de la Junta de Gobierno del Colegio de Registradores, o recabará su autorización en aquellas materias cuya competencia esté reservada al máximo órgano de gobierno de los Registradores.

El Comité técnico de Asesoramiento y Cumplimiento Normativo realizará, al menos, una revisión anual de los documentos de la Declaración de Prácticas de Certificación y de las Políticas de Certificación del PSC del CORPME.

1.5.2. Procedimiento de aprobación y modificación de la Declaración de Prácticas de Certificación.

La aprobación y subsiguientes modificaciones de la presente PC, corresponde en exclusiva a la Comisión Directora, en virtud de las facultades delegadas por la Junta de Gobierno del CORPME, de conformidad con las disposiciones del Reglamento interno del PSC.

Cualquier modificación en la presente PC será introducida y publicada en la página Web del CORPME (**http://pki.registradores.org/normativa/index.htm**). Los suscriptores disconformes con las modificaciones introducidas, podrán solicitar la revocación de su certificado digital.

La revocación interesada y voluntaria por el usuario disconforme con las disposiciones incorporadas con carácter sobrevenido a esta PC, no otorgará al suscriptor ningún derecho a ser compensado por tal motivo.

1.6. DATOS DE CONTACTO

Para consultas o comentarios relacionados con la presente PC el interesado deberá dirigirse al CORPME a través de alguno de los siguientes medios:

Colegio de Registradores de la Propiedad, Mercantiles y de Bienes muebles de España
Prestador del Servicio de Certificación del Colegio de Registradores
C/ DIEGO DE LEON, 21
28006-MADRID
Email: psc@registradores.org
Tlf: 902181442 o 912701699

1.7. DEFINICIONES Y ACRÓNIMOS

1.7.1. Definiciones

Agencia Española de Protección de Datos: Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada cuya finalidad es velar por el cumplimiento de la legislación sobre protección de datos personales

Autoridad de Certificación: es aquella persona física o jurídica que, de conformidad con la legislación sobre Firma Electrónica expide Certificados electrónicos, pudiendo prestar además otros servicios en relación con la Firma Electrónica.

Autoridad de Registro: entidad, con la que CORPME ha establecido un convenio, que realiza la comprobación de la identidad de los Solicitantes y Suscriptores de Certificados, y en su caso de la vigencia de facultades de representantes y subsistencia de la personalidad jurídica o de la representación voluntaria

Cadena de certificación: lista de Certificados que contiene al menos un Certificado y el Certificado raíz de CORPME

Certificado: documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula al Suscriptor unos Datos de verificación de Firma y confirma su identidad. En la presente Política de Certificación, cuando se haga referencia a Certificado se entenderá realizada a un Certificado emitidos por cualquier Autoridad de Certificación de CORPME

Certificado raíz: Certificado cuyo Suscriptor es una Autoridad de Certificación perteneciente a la jerarquía de CORPME como Prestador de Servicios de Certificación, y que contiene los Datos de verificación de Firma de dicha Autoridad firmado con los Datos de creación de Firma de la misma como Prestador de Servicios de Certificación

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten

Clave: secuencia de símbolos

Datos de creación de Firma (Clave Privada): son datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la Firma Electrónica

Datos de verificación de Firma (Clave Pública): son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma Electrónica

Declaración de Prácticas de Certificación (DPC): declaración de CORPME puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de Prestador de Servicios de Certificación en cumplimiento de lo dispuesto por la Ley

Dispositivo seguro de creación de Firma: instrumento que sirve para aplicar los Datos de creación de Firma cumpliendo con los requisitos establecidos en el Anexo III de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, y con lo establecido en las normas específicas de aplicación en España

Directorio de Certificados: repositorio de información que sigue el estándar X.500 del ITU-T

Documento electrónico: conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información

Documento de seguridad: documento exigido por la LOPD cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por CORPME como Prestador de Servicios de Certificación, para la protección de los datos de carácter personal contenidos en los Ficheros de la actividad de certificación que contienen datos personales (en adelante los Ficheros).

Encargado del Tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del Responsable del tratamiento de los Ficheros

Firma Electrónica reconocida: es aquella Firma Electrónica avanzada basada en un Certificado reconocido y generada mediante un Dispositivo seguro de creación de Firma

Firma Electrónica avanzada: es aquella Firma Electrónica que permite establecer la identidad personal del Suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al Suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que éste puede mantener bajo su exclusivo control

Firma Electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una Función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales

Infraestructura de Claves Públicas (PKI, Public key Infrastructure): infraestructura que soporta la gestión de Claves Públicas para los servicios de autenticación, cifrado, integridad, o no repudio

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal: ley que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar

Listas de Revocación de Certificados o Listas de Certificados Revocados (CRL): lista donde figuran exclusivamente las relaciones de Certificados revocados o suspendidos (no los caducados)

Módulo Criptográfico Hardware de Seguridad (HSM): módulo hardware utilizado para realizar funciones criptográficas y almacenar Claves en modo seguro. -Número de serie de Certificado: valor entero y único que está asociado inequívocamente con un Certificado expedido por CORPME

OCSP (Online Certificate Status Protocol): protocolo informático que permite la comprobación del estado de un Certificado en el momento en que éste es utilizado

OCSP Responder: servidor informático que responde, siguiendo el protocolo OCSP, a las Peticiones OCSP con el estado del Certificado por el que se consulta

OID (Object IDentifier): valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID

Petición OCSP: petición de consulta de estado de un Certificado a OCSP Responder siguiendo el protocolo OCSP

PIN: (Personal Identification Number) número específico sólo conocido por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo

Prestador de Servicios de Certificación: es aquella persona física o jurídica que, de conformidad con la legislación sobre Firma Electrónica expide Certificados electrónicos, pudiendo prestar además otros servicios en relación con la Firma Electrónica. En la presente Política de Certificación, se corresponderá con las Autoridades de Certificación pertenecientes a la jerarquía de CORPME

Política de Certificación (PC): documento que completa la Declaración de Prácticas de Certificación, estableciendo las condiciones de uso y los procedimientos seguidos por CORPME para emitir Certificados

Póliza: a efectos de la presente Política de Certificación se entenderá por la Póliza el documento notarial que el Notario autoriza ante el Suscriptor de un Certificado que documenta la intervención notarial como Autoridad de Registro, así como su intervención en el caso de revocación del mismo

PKCS#10 (Certification Request Syntax Standard): estándar desarrollado por RSA Labs, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de Certificado

PUK: (Personal Unblocking Key) número o clave específica sólo conocido por la persona que tiene que acceder a un recurso que se utiliza para desbloquear el acceso a dicho recurso

Responsable del Fichero (o del Tratamiento del Fichero): persona que decide sobre la finalidad, contenido y uso del tratamiento de los Ficheros. -Responsable de Seguridad: encargado de coordinar y controlar las medidas que impone el Documento de seguridad en cuanto a los Ficheros

SHA-1: Secure Hash Algorithm (algoritmo seguro de resumen –hash-). Desarrollado por el NIST y revisado en 1994 (SHA-1). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para asegurar la Integridad de los documentos durante el proceso de Firma Electrónica

Sellado de Tiempo: constatación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones Request For Comments: 3161 – "Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP)", que logra datar el documento de forma objetiva

Solicitante: persona física que previa identificación, solicita la emisión de un Certificado

Suscriptor (o Subject): el titular o firmante del Certificado. La persona cuya identidad personal queda vinculada mediatamente a los datos firmados electrónicamente, a través de una Clave Pública certificada por el Prestador de Servicios de Certificación. El concepto de Suscriptor, será referido en

los Certificados y en las aplicaciones informáticas relacionadas con su emisión como Subject, por estrictas razones de estandarización internacional

Tarjeta criptográfica: tarjeta utilizada por el Suscriptor para almacenar claves privadas de firma y descifrado, para generar firmas electrónicas y descifrar mensajes de datos. Tiene la consideración de Dispositivo seguro de creación de Firma de acuerdo con la Ley y permite la generación de Firma Electrónica reconocida

Terceros que confían en Certificados: aquellas personas que depositan su confianza en un Certificado de CORPME, comprobando la validez y vigencia del Certificado según lo descrito en esta Declaración de Prácticas de Certificación

UIT (Unión Internacional de Telecomunicaciones): organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones

X.500: estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525

X.509: estándar desarrollado por la UIT, que define el formato electrónico básico para Certificados electrónicos

1.7.2. Acrónimos

AAP: Autoridad de Aprobación de Políticas

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500

CA: Certification Authority (Autoridad de Certificación).

CDP: CRL Distribution Point (Punto de Distribución de CRL).

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CP: Certificate Policy (Política de Certificación).

CPS: Certification Practice Statement (Declaración de Prácticas de Certificación)

CORPME: Colegio de Registradores de la Propiedad, Mercantiles y de Bienes muebles de España

CRL: Certificate Revocation List (Lista de Revocación de Certificados)

CSR: Certificate Signing Request (petición de certificado). Conjunto de datos, que contienen una clave pública y su Firma Electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública.

CWA: CEN Workshop Agreement

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de un directorio X.500

FIPS: Federal Information Processing Standard

HSM: Hardware Security Module. Módulo de seguridad criptográfica empleado para el almacenamiento de claves y realización de operaciones criptográficas seguras

IANA: Internet Assigned Numbers Authority

IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)

ITU: International Telecommunication Union

O: Organisation (Organización). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500

OCSP: Online Certificate Status Protocol. Protocolo para la verificación online de la validez de un certificado electrónico

OID: Object Identifier (Identificador Único de Objeto)

OU: Organisational Unit (Unidad Organizativa). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500

PSC: Proveedor de Servicios de Certificación

PIN: Personal Identification Number (Número de Identificación Personal). Password que protege el acceso a un dispositivo criptográfico

PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por los laboratorios de **RSA** aceptados internacionalmente

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

PUK: PIN Unlock Key. Password que permite desbloquear un dispositivo criptográfico bloqueado por haber introducido en repetidas ocasiones un PIN erróneo de forma consecutiva

RA: Registration Authority (Autoridad de Registro)

RFC: Request For Comments. Standard desarrollado por el IETF

ROA: Real Observatorio de la Armada Española

SSI: Servicio de Sistemas de Información del Colegio de Registradores

SSL: Secure Sockets Layer (Capa de Conexión Segura)

TSA: TimeStamp Authority (Autoridad de Sellado de Tiempo)

TST: TimeStamp Token (Token de Sellado de Tiempo)

TSU: TimeStamp Unit (Unidad de Sellado de Tiempo)

UTC: Universal Time Coordinated

VA: Validation Authority (Autoridad de Validación)

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. DIRECTORIO DE VALIDACIÓN DE CERTIFICADOS

El CORPME mantiene un Directorio de Validación de Certificados permanentemente disponible y accesible a cualquier interesado, de conformidad con la normativa vigente. Para garantizar un acceso continuado y sin disrupciones al servicio de verificación de certificados, el Servidor de directorio está duplicado y balanceado, de tal forma que en caso de fallo o caída del servicio, el segundo directorio será inmediatamente puesto en línea garantizándose de este modo la disponibilidad del mismo.

El Directorio de Validación de Certificados es un directorio público de consulta, en el que se encuentran todas las Listas de Certificados Revocados (CRL's) emitidas por el Prestador del Servicio de Certificación, cuyo plazo de caducidad aún no ha vencido, que incluyen la fecha y hora en el que tuvo lugar la revocación. No se establecerán más limitaciones de acceso al Directorio que las impuestas por razones de seguridad.

ARL	**http://pki.registradores.org/crls/arl_scr.crl**
CRL CA Certificados Internos	**http://pki.registradores.org/crls/crl_int_scr.crl**
CRL CA Certificados Externos	**http://pki.registradores.org/crls/crl_ext_scr.crl**
Servicio de validación en línea que implementa el protocolo OCSP	**http://ocsp.registradores.org y https://ocsp.registradores.org**
Servicio de Sello de Tiempo (Time Stamping Protocol)	**http://tsa.registradores.org y https://tsa.registradores.org**
Certificado Autoridad Certificadora CORPME	**http://pki.registradores.org/certificados/ca_raiz_scr.crt**
Certificado CA Internos	**http://pki.registradores.org/certificados/ca_int_scr.crt**
Certificado CA Externos	**http://pki.registradores.org/certificados/ca_ext_scr.crt**
Prácticas y Políticas de Certificación	**http://pki.registradores.org/normativa/index.htm**

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El Directorio se publica de acuerdo con el estándar LDAP (Lightweight Directory Access Protocol) y dispondrá de la ARL publicada y las CRL's publicadas, que siguen la norma correspondiente (Certificate Revocation List, versión 2) del estándar X.509. También podrá utilizarse el estándar OCSP (Online Certificate Status Protocol).

Las listas de certificados revocados se actualizarán con la periodicidad indicada en el apartado 4.9.7 del presente documento.

2.3. FRECUENCIA DE PUBLICACIÓN

La DPC y las Políticas de Certificación se publicarán en el momento de su creación y se volverán a publicar en el momento en que se apruebe cualquier modificación sobre las mismas. Las modificaciones se harán públicas en el Directorio web referenciado en el apartado 2.1 del presente documento.

La CA añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el apartado 4.9.7 del presente documento.

2.4. CONTROLES DE ACCESO A LA INFORMACIÓN DE CERTIFICACIÓN

El acceso para la consulta de la DPC y PCs es público para todo interesado que lo desee. El CORPME dispondrá de las medidas de seguridad necesarias para evitar la manipulación no autorizada de estos documentos. Así mismo, estarán firmados digitalmente mediante un certificado emitido del CORPME para garantizar su integridad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

3.1.1. Tipos de nombres

Todos los titulares de certificados requieren un nombre distintivo (Distinguished Name) conforme con el estándar X.500.

3.1.1.1. Certificado Reconocido de Registrador

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Nombre del registro>	Nombre del registro en el que es titular, interno o accidental
CN	NOMBRE apellidos nombre – NIF nif	Todos los datos deben ir en MAYÚSCULAS

3.1.1.2. Certificado Reconocido de Personal Interno

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Unidad de Destino>	
CN	NOMBRE apellidos nombre – NIF nif, nie, pasaporte u otros	Todos los datos deben ir en MAYÚSCULAS

3.1.1.3. Certificado No Reconocido para Procedimientos Registrales

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Nombre del Registro titular del certificado>	Nombre del Registro
CN	<Nombre del Registro titular del certificado>	Nombre del Registro

3.1.1.4. Certificado No Reconocido de Servidor de SSL

La estructura del certificado, referente a la extensión *subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País
O	Colegio de Registradores de la Propiedad y Mercantiles de España	Organización
OU	<Departamento, Empresa o Entidad final>	Nombre del Departamento, Empresa o Entidad final destinataria
CN	<Nombre del Dominio>	Nombre del Dominio

3.1.2. Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos de los titulares de los certificados deben ser significativos, ajustándose a las normas impuestas en el apartado anterior.

3.1.3. Reglas para interpretar varios formatos de nombres

La regla utilizada por el PSC del CORPME para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.4. Unicidad de los nombres

El conjunto de nombre distintivo (Distinguished Name) más el contenido de la extensión *Policy Identifier* debe ser único y no ambiguo.

- Para Certificados Reconocidos de Registrador, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF en el CN garantiza la unicidad del mismo.
- Para Certificados Reconocidos de Personal Interno, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF, NIE, pasaporte u otro documento identificativo en el CN garantiza la unicidad del mismo.

- Para Certificado No Reconocido de Procedimientos Registrales, el uso del nombre del registro emisor en el OU y del nombre del registro titular del certificado en el CN, garantiza la unicidad del mismo.
- Para Certificado No Reconocido de Servidor de SSL, el uso del Departamento en el OU y del nombre del dominio en el CN, garantiza la unicidad del mismo.

3.1.5. Procedimientos de resolución de conflictos sobre nombres

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto 9.13 del presente documento.

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas

No estipulado.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. Medio de prueba de posesión de la clave privada

Las claves de los certificados internos:

- Certificado Reconocido de Registrador
- Certificado Reconocido de personal interno

Serán generadas por el dispositivo criptográfico seguro del solicitante estando bajo la custodia de éste, por lo que, la posesión de la clave privada correspondiente a la clave pública para la que el solicitante solicita que se genere el certificado, quedará probada mediante el envío de la petición de firma del certificado (CSR).

Para los Certificados no Reconocidos de servidor SSL el CORPME comprobará que el solicitante posee la clave privada correspondiente a la clave pública para la que solicita que se genere el certificado.

Para los Certificados no Reconocidos para Procedimientos Registrales, el CORPME comprobará mediante la recepción de la licencia de uso firmada por el titular del registro correspondiente, que el solicitante posee la clave privada correspondiente a la clave pública para la que solicita que se genere el certificado.

3.2.2. Autenticación de la identidad de una persona jurídica

No estipulado.

3.2.3. Autenticación de la identidad de una persona física

El solicitante deberá proporcionar la siguiente información, en función del certificado que solicite:

3.2.3.1. Certificado Reconocido de Registrador

- Nombre del registro (registro en el que ejerce su función el titular del certificado).
- Nombre y apellidos y documento identificativo (NIF) del suscriptor
- Correo electrónico
- Dirección postal
- Nombre Principal de Windows (UPN)

3.2.3.2. Certificado Reconocido de Personal Interno

- Unidad de destino (en el que ejerce su función el titular del certificado), salvo para los aspirantes, jubilados o excedentes, cuya unidad de destino corresponderá a la Unidad de Tramitación Central.
- Nombre y apellidos y documento identificativo (NIF, NIE, pasaporte u otros) del suscriptor
- Correo electrónico
- Dirección postal
- Nombre Principal de Windows (UPN)
- Subtipo: Registro, Colegio, Decanato, Sociedad del Colegio o empleados en situaciones especiales
- Sociedad, si el subtipo es Sociedad del Colegio
- Situación del registrador: Aspirante, Jubilado o Excedente

3.2.4. Autenticación de la identidad de un dispositivo

3.2.4.1. Certificado no Reconocido para Procedimientos Registrales

- Nombre del registro titular del certificado
- Correo electrónico
- Dirección postal

3.2.4.2. Certificado no Reconocido de servidor SSL

- Nombre del Dominio
- Correo electrónico
- Dirección postal

3.2.5. Información no verificada sobre el solicitante

No estipulado.

3.2.6. Comprobación de las facultades de representación

No estipulado.

3.2.7. Criterios para operar con CA externas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN

La identificación y autenticación de los titulares de los certificados para las solicitudes de renovación por cualquier motivo, que se encuentran especificados en el apartado 4.7 del presente documento, se realizará a través del proceso de emisión de certificados, es decir, mediante el NIF, NIE, pasaporte u otro documento identificativo del titular.

Además, el Operador de la Unidad de Tramitación correspondiente, solicitará la documentación acreditativa del atributo certificable de que se trate en virtud del Tipo de Certificado, salvo para los Certificados Reconocidos de representante de persona jurídica, donde el Operador confirmará por sus medios la documentación acreditativa del solicitante.

De igual manera, las Unidades de Tramitación serán responsables del archivado de toda documentación relacionada con los certificados y sus solicitudes, debiendo archivarse por un mínimo de quince (15) años.

Para los Certificados Internos no Reconocidos (Procedimientos Registrales y SSL), la Unidad de Tramitación Central notificará al titular por correo electrónico corporativo la futura expiración del certificado, con al menos un mes de antelación a la fecha en que se produzca.

Siempre bajo petición del titular del certificado del dispositivo, la Unidad de Tramitación Central procederá a la emisión de un nuevo certificado con un contenido equivalente al del que va a caducar y lo enviará a su titular mediante correo electrónico corporativo, con antelación suficiente para evitar la interrupción del servicio.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

La identificación y autenticación de los titulares de los certificados para las solicitudes de revocación por cualquier motivo, que se encuentran especificados en el apartado 4.9 del presente documento, se realizará mediante el NIF, NIE, pasaporte u otro documento identificativo del titular.

Para los Certificados Internos no Reconocidos (Procedimientos Registrales y SSL), la Unidad de Tramitación Central identificará al titular mediante el correo electrónico corporativo utilizado en la solicitud del certificado.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede efectuar una solicitud

La solicitud variaría en función del tipo de Certificado Reconocido solicitado, a continuación se diferencia el procedimiento según el tipo solicitado:

4.1.1.1. Certificado Reconocido de Registrador

En el presente caso, no es necesaria la petición de cita a través de la página web para la comparecencia.

El Registrador solicitante deberá comparecer ante la Unidad de Tramitación correspondiente al Registro del que haya tomado posesión, en un plazo no superior a tres días desde la toma de posesión del Registro, aportando un documento identificativo (NIF, NIE, pasaporte u otro) y copia original del nombramiento.

La Unidad de Tramitación dispondrá de los medios necesarios para comprobar la condición de registrador del solicitante y de la situación de servicio activo del mismo, consultándolo en la Guía colegial para comprobarlo.

El procedimiento de emisión se realizará de acuerdo con las siguientes fases:

1. **Solicitud**: El Registrador se persona en la Unidad de Tramitación de los Registros con su NIF o pasaporte. El Operador del Registro correspondiente introducirá los datos de la solicitud en la aplicación y comprobará si existe algún certificado vigente de la misma clase al que se pretende expedir y a nombre del mismo titular y, de ser así, procederá a su revocación.
2. **Aceptación de la solicitud y de la licencia**: se imprimirán dos copias de la licencia de uso, y de la solicitud de revocación, en los casos que proceda, que firmará el solicitante.
3. **Generación de claves y asignación de contraseñas**: la Unidad de Tramitación correspondiente entregará al suscriptor un dispositivo criptográfico sin inicializar y este introducirá la contraseña de acceso y ordenará la generación de las claves dentro del dispositivo criptográfico. El suscriptor deberá introducir personalmente la contraseña de acceso al dispositivo criptográfico, de modo que esta no sea conocida en ningún momento por el CORPME.

   El Registrador al frente de la Unidad de Tramitación correspondiente certificará que la firma ha sido creada con la intervención personal del solicitante, generándose la clave privada en el interior del dispositivo criptográfico (la autoridad de registro – el registrador - introducirá personalmente las contraseñas que dan acceso al sistema de generación de certificados y requiriendo al solicitante la introducción de la clave de acceso al dispositivo que protege la clave privada del certificado), así como que éste acepta los requisitos de asunción de la firma electrónica.
4. **Emisión e instalación del certificado**: la solicitud de certificado, conteniendo la clave pública, se enviará telemáticamente a la Unidad Técnica, que remitirá inmediatamente el certificado. A continuación, el certificado se introducirá en el dispositivo criptográfico.

Una copia de la solicitud y de la licencia quedará en poder del titular y la otra será archivada en la Unidad de Tramitación, junto a la referida certificación y, por un periodo de quince (15) años.

4.1.1.2. Certificado Reconocido de Personal Interno

En el presente caso, no es necesaria la petición de cita a través de la página web para la comparecencia.

El solicitante, empleado del Colegio o de los Registros, deberá comparecer ante la Unidad de Tramitación de los Registros correspondiente, aportando un documento identificativo (NIF, NIE, pasaporte u otros).

El procedimiento de emisión se realizará de acuerdo con las siguientes fases:

1. **Solicitud**: El solicitante del certificado se persona en la Unidad de Tramitación con su NIF, NIE, pasaporte u otro. El Operador del Registro correspondiente introducirá los datos de la solicitud y comprobará si existe algún certificado vigente de la misma clase al que se pretende expedir y a nombre del mismo titular y, de ser así, procederá a su revocación.
2. **Aceptación de la solicitud y de la licencia**: se imprimirán dos copias de la licencia de uso, y de la solicitud de revocación, en los casos que proceda, que firmará el solicitante.
3. **Generación de claves y asignación de contraseñas**: la Unidad de Tramitación correspondiente entregará al suscriptor un dispositivo criptográfico sin inicializar y este introducirá la contraseña de acceso y ordenará la generación de las claves dentro del dispositivo criptográfico. El suscriptor deberá introducir personalmente la contraseña de acceso al dispositivo criptográfico, de modo que esta no sea conocida en ningún momento por el CORPME.

   El Registrador al frente de la Unidad de Tramitación correspondiente certificará que la firma ha sido creada con la intervención personal del solicitante, generándose la clave privada en el interior del dispositivo criptográfico (el registrador introducirá personalmente las contraseñas que dan acceso al sistema de generación de certificados y requiriendo al solicitante la introducción de la clave de acceso al dispositivo que protege la clave privada del certificado), así como que éste acepta los requisitos de asunción de la firma electrónica.
4. **Emisión e instalación del certificado**: la solicitud de certificado, conteniendo la clave pública, se enviará telemáticamente a la Unidad Técnica, que remitirá inmediatamente el certificado. A continuación, el certificado se introducirá en el dispositivo criptográfico.

Una copia de la solicitud y de la licencia quedará en poder del titular y la otra será archivada en la Unidad de Tramitación, junto a la referida certificación y, por un periodo de quince (15) años.

4.1.1.3. Certificado No Reconocido para Procedimientos Registrales

Los Certificados no Reconocidos para Procedimientos registrales serán emitidos desde la Unidad de Tramitación Central. Se generarán lotes de emisión de certificados y una vez generados se ejecutará un script para cambiar la contraseña de los PKCS #12 con una contraseña aleatoria y única para cada uno de ellos.

Desde los servicios centrales del CORPME se procederá a instalar los certificados en los servidores de integración de cada registro y una vez finalizada la operación se notificará la contraseña del PKCS #12 al responsable de seguridad del registro para que procedan a la instalación del mismo en los puestos clientes del registro.

Pasado el periodo de una semana se procederá a la revocación de los certificados que han sido renovados.

La Unidad de Tramitación Central, una vez que los certificados hayan sido instalados, borrará cualquier referencia a éstos y sus respectivas contraseñas, para garantizar el no repudio.

4.1.1.4. Certificado No Reconocido de Servidor de SSL

Para la emisión de certificados no reconocidos de servidor de SSL se deberá enviar una solicitud mediante correo electrónico corporativo a la Unidad de Tramitación Central del CORPME.

La Unidad de Tramitación Central procederá a dar trámite a la solicitud del certificado, validando esta solicitud el Director Técnico del SSI y comprobando si existe otro certificado de la misma clase y a nombre del mismo titular y, de ser así, proceder a la denegación de la solicitud. Finalmente la Unidad de Tramitación Central notificará al solicitante la aprobación o denegación de la solicitud del certificado.

En caso que la validación de la solicitud haya sido favorable, se proporcionará el certificado emitido, y se le remitirá la licencia de uso por duplicado, en formato electrónico, debiendo firmar ambas el solicitante y devolver uno de los ejemplares. Una copia de la solicitud y de la licencia quedará en poder del titular y la otra será archivada en la Unidad de Tramitación Central, por un periodo de quince (15) años.

4.1.2. Registro de las solicitudes de certificados y responsabilidades de los solicitantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2. TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2.2. Aprobación o denegación de las solicitudes de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.2.3. Plazo para la tramitación de las solicitudes de certificados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3. EMISIÓN DE CERTIFICADOS

4.3.1. Actuaciones de la CA durante la emisión del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.3.2. Notificación al solicitante de la emisión por la CA del certificado

En las solicitudes de los certificados en las que se incluya el correo electrónico del interesado, se enviará un email notificando al solicitante la emisión del certificado por parte de la CA. Este email solamente será a título informativo. Esta notificación es aplicable a los siguientes certificados:

- Certificados Reconocidos de registrador.
- Certificados Reconocidos para personal interno.
- Certificados no Reconocidos para procedimientos registrales.
- Certificados no Reconocidos de servidor de SSL.

4.3.3. Licencia de Uso

4.3.3.1. Certificado Reconocido de Registrador

La firma de la licencia de uso del certificado implicará la aceptación del mismo, de la DPC y de la presente PC. Incluirá necesariamente los siguientes contenidos:

- **Los datos personales del Registrador**: nombre y apellidos, Registro donde desempeña su función, teléfono y dirección de correo electrónico.
- **Una declaración del Registrador** en la que manifiesta haber generado en el dispositivo criptográfico la clave privada y recibido ésta con el certificado y en la que se compromete a utilizar ésta de acuerdo con lo dispuesto en la DPC, el Reglamento interno del PSC y la presente PC.

El consentimiento del solicitante para la cesión de sus datos de carácter personal al CORPME en la medida en que sean necesarios para que éste preste los servicios de certificación. Estos datos se mantendrán confidencialmente en el CORPME, y nunca serán cedidos a terceros.

4.3.3.2. Certificado Reconocido de Personal Interno

La firma de la licencia de uso del certificado implicará la aceptación del mismo, de la DPC y de la PC correspondiente. Incluirá necesariamente los siguientes contenidos:

- **Los datos personales** del personal interno: nombre y apellidos, Registro, Decanato, Colegio o Sociedades Colegiales donde desempeña su función, teléfono y dirección de correo electrónico.
- **Una declaración** del personal interno en la que manifiesta haber generado en el dispositivo criptográfico la clave privada y recibido ésta con el certificado y en la que se compromete a utilizar ésta de acuerdo con lo dispuesto en la DPC, en el Reglamento del SCR y en la PC.
- **El consentimiento del solicitante** para la cesión de sus datos de carácter personal al CORPME en la medida en que sean necesarios para que éste preste los servicios de certificación. Estos datos se mantendrán confidencialmente en el CORPME, y nunca serán cedidos a terceros.

4.3.3.3. Certificado No Reconocido para Procedimientos Registrales

La firma de la licencia de uso del certificado será firmada por el titular del registro correspondiente e implicará la aceptación del mismo, de la DPC y de la presente PC. Una vez firmada, la licencia será remitida a la Unidad de Tramitación Central e incluirá necesariamente los siguientes contenidos:

- Los datos personales del titular: nombre y apellidos del titular, nombre oficial del Registro destino, teléfono y dirección de correo electrónico.
- Una declaración del titular en la que manifiesta haber recibido el certificado y en la que se compromete a utilizar de acuerdo con lo dispuesto en el Reglamento y en las presentes Condiciones de Certificación.
- El consentimiento del solicitante para la cesión de sus datos de carácter personal al Servicio en la medida en que sean necesarios para que éste preste los servicios de certificación.

La licencia firmada quedará archivada en la Unidad de Tramitación Central durante quince (15) años.

4.3.3.4. Certificado No Reconocido de Servidor de SSL

El solicitante deberá firmar la licencia de uso del certificado, aceptando el mismo y de las presentes Condiciones de Certificación. La licencia incluirá necesariamente los siguientes contenidos:

- Los datos personales del Solicitante: nombre y apellidos del Solicitante, Departamento, Empresa o Entidad final a la que pertenece, dirección de correo electrónico, y la dirección (URL) de la máquina donde va a instalarse.

- Una declaración del Solicitante en la que manifiesta haber recibido el certificado y en la que se compromete a utilizar de acuerdo con lo dispuesto en el Reglamento y en las presentes Condiciones de Certificación.
- El consentimiento del solicitante para la cesión de sus datos de carácter personal al Servicio en la medida en que sean necesarios para que éste preste los servicios de certificación.

La licencia firmada quedará archivada en la Unidad de Tramitación Central durante quince (15) años.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Mecanismo de aceptación del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.4.2. Publicación del certificado por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Uso de la clave privada y del certificado por el titular

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.5.2. Uso de la clave pública y del certificado por los terceros aceptantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.6. RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

4.6.1. Circunstancias para la renovación de certificados sin cambio de claves

No estipulado.

4.6.2. Quién puede solicitar la renovación de los certificados sin cambio de claves

No estipulado.

4.6.3. Tramitación de las peticiones de renovación de certificados sin cambio de claves

No estipulado.

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

No estipulado.

4.6.5. Forma de aceptación del certificado sin cambio de claves

No estipulado.

4.6.6. Publicación del certificado sin cambio de claves por la CA

No estipulado.

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

No estipulado.

4.7. RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Los certificados digitales que emite el CORPME son susceptibles de renovación siempre con cambio de claves. Caducado o extinguido un certificado digital, por agotarse el periodo de vigencia del mismo o por concurrir alguna de las causas de extinción recogidas en la Declaración de Practicas de Certificación del CORPME, únicamente cabrá solicitar un nuevo certificado digital. El procedimiento será el mismo que para la emisión de un nuevo certificado.

De todas formas, la Unidad de Tramitación Central notificará al suscriptor por correo electrónico la futura expiración de los certificados, con al menos dos (2) meses de antelación a la fecha en que se produzca, indicando al suscriptor los pasos a seguir para la obtención de un nuevo certificado.

La solicitud de renovación del certificado puede ser:

- **Presencial**: Se tratará igual que una emisión inicial.
- **No presencial**: Se aplica a usuarios con un certificado activo, dentro del período de renovación definido como dos (2) meses antes de la fecha de caducidad del certificado. Únicamente se permitirá realizar una renovación no presencial una vez, la siguiente el usuario está obligado a renovar presencialmente su certificado, según dicta la normativa de firma digital.

4.7.1. Circunstancias para una renovación con cambio claves de un certificado

Algunos de los motivos, entre otros, por los que se puede renovar un certificado son:

- Expiración del periodo de validez.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de las mismas.
- Cambio de formato.

Todas las renovaciones de certificados del PSC del CORPME se realizarán con cambio de claves.

4.7.2. Quién puede pedir la renovación de los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.7.3. Tramitación de las peticiones de renovación de certificados con cambio de claves

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.7.5. Forma de aceptación del certificado con las claves cambiadas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.7.6. Publicación del certificado con las nuevas claves por la CA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.8. MODIFICACIÓN DE CERTIFICADOS

Se habla de modificación de un certificado cuando se emite uno nuevo debido a cambios en la información del certificado no relacionados con su clave pública o expiración del periodo de validez.

Las modificaciones de los certificados pueden venir dadas por diferentes motivos tales como:

- Cambio de nombre.
- Cambio en las funciones dentro de la organización.
- Reorganización como resultado del cambio en el nombre distintivo.

Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán como una renovación de certificados, por lo que son de aplicación los apartados anteriores al respecto.

4.8.1. Circunstancias para la modificación de un certificado

No estipulado.

4.8.2. Quién puede solicitar la modificación de los certificados

No estipulado.

4.8.3. Tramitación de las peticiones de modificación de certificados

No estipulado.

4.8.4. Notificación de la emisión de un certificado modificado al titular

No estipulado.

4.8.5. Forma de aceptación del certificado modificado

No estipulado.

4.8.6. Publicación del certificado modificado por la CA

No estipulado.

4.8.7. Notificación de la modificación del certificado por la CA a otras Autoridades

No estipulado.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

4.9.1. Circunstancias para la revocación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.2. Quién puede solicitar la revocación

Solamente podrá solicitar la revocación de los certificados el titular de los mismos. Para el caso particular de los Certificados no Reconocidos SSL, la revocación se solicitará mediante el representante de los mismos.

4.9.3. Procedimiento de solicitud de revocación

La revocación puede hacerse de dos formas:

- **Forma presencial**: Para solicitar la revocación del certificado de forma presencial el suscriptor deberá personarse ante la Unidad de Tramitación Central o ante aquella que emitió el certificado. El operador comprobará la identidad del solicitante y procederá a la revocación del certificado, guardando la solicitud de revocación firmada durante quince (15) años.
- **Forma remota**: Por causa de urgencia mediante una llamada telefónica a su Servicio de Asistencia Telefónica, como así queda recogido en el procedimiento interno que dispone el CORPME. Igualmente la revocación se podrá realizar firmando una solicitud electrónica de revocación con certificado reconocido vigente del mismo titular.

La revocación se realizará de forma automática, bajo la única responsabilidad del suscriptor.

4.9.4. Periodo de gracia de la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.5. Plazo en el que la CA debe resolver la solicitud de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.6. Requisitos de verificación de las revocaciones por los terceros que confían

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.7. Frecuencia de emisión de CRL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.8. Tiempo máximo entre la generación y la publicación de las CRL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.9. Disponibilidad de un sistema en línea de verificación del estado de los certificados

Además de la publicación de las CRL's, el CORPME dispone de un servicio OCSP de validación de certificados, que implementa la *"RFC6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol"*, en los que se puede consultar el estado de revocación de un determinado certificado emitido por el PSC del CORPME. La dirección URL de acceso se encuentra publicada en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.10. Requisitos de comprobación en línea de revocación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.11. Otras formas de divulgación de información de revocación disponibles

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.12. Requisitos especiales de revocación de claves comprometidas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.13. Causas para la suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.14. Quién puede solicitar la suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.15. Procedimiento para la solicitud de suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.9.16. Límites del periodo de suspensión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1. Características operativas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.10.2. Disponibilidad del servicio

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.10.3. Características adicionales

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.11. EXTINCIÓN DE LA VALIDEZ DE UN CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

No estipulado.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

No estipulado.

5. CONTROLES DE SEGURIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1. SEGURIDAD FÍSICA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.1. Ubicación y medidas de seguridad física de las instalaciones de CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.2. Acceso físico

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.3. Suministro eléctrico y acondicionamiento ambiental de las instalaciones del CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.4. Exposición al agua

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.5. Medidas contra incendios e inundaciones.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.6. Sistema de almacenamiento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.7. Eliminación de residuos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.1.8. Política de Respaldo de Información.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2. CONTROLES DE PROCEDIMIENTO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2.1. Roles responsables del control y gestión de la PKI del CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2.2. Número de personas requeridas por tarea

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.2.3. Roles que requieren segregación de funciones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3. CONTROLES DE PERSONAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.1. Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.2. Procedimientos de comprobación de antecedentes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.3. Requerimientos de formación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.4. Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.5. Frecuencia y secuencia de rotación de tareas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.6. Sanciones por actuaciones no autorizadas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.7. Requisitos de contratación de terceros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.3.8. Documentación proporcionada al personal

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.1. Tipos de eventos registrados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.2. Frecuencia de procesado de registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.3. Periodo de conservación de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.4. Protección de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.5. Procedimientos de respaldo de los registros de auditoría

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.7. Notificación al sujeto causa del evento

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.4.8. Análisis de vulnerabilidades

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5. ARCHIVADO DE REGISTROS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5.1. Tipo de eventos archivados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5.2. Periodo de conservación de registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5.3. Protección del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5.4. Procedimientos de copia de respaldo del archivo

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5.5. Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.5.7. Procedimientos para obtener y verificar información archivada

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.6. CAMBIO DE CLAVES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.7. RECUPERACIÓN ANTE COMPROMISO DE CLAVE O CATÁSTROFE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.7.1. Procedimientos de gestión de incidentes y compromisos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.7.3. Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.8. CESE DE UNA CA O RA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.8.1. Autoridad de Certificación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

5.8.2. Autoridad de Registro

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. Generación del par de claves

Las claves de suscriptor, que tendrán una longitud de 1024 bits, excepto para la longitud de las claves certificadas para los Certificados SSL que es de 2048 bits,

Para los Certificados Reconocidos (Registradores y Personal interno) son generadas siempre durante la comparecencia del solicitante y con su intervención personal en el proceso de asignación de claves.

Para los Certificados no Reconocidos (Procedimientos Registrales y SSL) no es necesaria la comparecencia personal del solicitante y se generarán las claves en el dispositivo y una petición de certificado que se facilitará a la Unidad de Tramitación Central.

6.1.2. Entrega de la clave privada al titular

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.1.3. Entrega de la clave pública al emisor del certificado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.1.4. Entrega de la clave pública de la CA a los terceros que confían

La clave pública de las CA del PSC del CORPME está a disposición de los terceros que confían en el directorio web del CORPME, definido en el apartado 2.1 de esta PC.

6.1.5. Tamaño de las claves

El tamaño de las claves de los certificados internos es de 1024 bits, salvo para los certificados SSL, que es de 2048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de los certificados internos está codificada de acuerdo con RFC6818.

6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para los certificados internos vienen dados por el valor de las extensiones *Key Usage* y *Extended Key Usage* de los mismos. El contenido de dichas extensiones para cada uno de los tipos de certificados externos se puede consultar en el apartado 7.1.2 del presente documento.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS

6.2.1. Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por las CA del PSC del CORPME cumplan con la certificación FIPS 140-2 de nivel 3.

6.2.2. Control multipersona (k de n) de la clave privada

Las claves privadas de los certificados internos no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el suscriptor.

6.2.3. Custodia de la clave privada

La custodia de las claves privadas de los certificados internos la realizan los propios titulares de las mismas.

6.2.4. Copia de seguridad de la clave privada

En ningún caso se realizarán copias de seguridad de las claves privadas de firma de los certificados internos para garantizar el no repudio.

6.2.5. Archivo de la clave privada

Las claves privadas de firma de los certificados internos nunca serán archivadas para garantizar el no repudio.

6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

En ningún caso es posible transferir las claves privadas de firma de los certificados internos para garantizar el no repudio.

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas de firma de los certificados internos se generan en el dispositivo criptográfico en el momento de la generación de los certificados.

6.2.8. Método de activación de la clave privada

La activación de la clave privada la podrá efectuar el titular de la misma mediante el uso de su PIN.

6.2.9. Método de desactivación de la clave privada

No estipulado

6.2.10. Método de destrucción de la clave privada

No estipulado

6.2.11. Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 nivel 3.

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 (DPC) del CORPME.

6.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves

El periodo de validez de los certificados internos es de dos (2) años desde el momento de emisión del mismo, salvo para los certificados SSL, que será bajo petición del solicitante entre una vigencia mínima de un (1) año, y una vigencia máxima de cinco (5) años.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de los datos de activación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.4.2. Protección de los datos de activación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.4.3. Otros aspectos de los datos de activación

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1. Requerimientos técnicos de seguridad específicos

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.5.2. Evaluación de la seguridad informática

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.6.1. Controles de desarrollo de sistemas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.6.2. Controles de gestión de seguridad

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.6.3. Controles de seguridad del ciclo de vida

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.7. CONTROLES DE SEGURIDAD DE LA RED

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

6.8. SELLADO DE TIEMPO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1. PERFIL DE CERTIFICADO

7.1.1. Número de versión

Los certificados están firmados electrónicamente por el CORPME con la clave privada correspondiente a la clase de los certificados internos y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

7.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- *Subject Key Identifier*
- *Certificate Policies*
- *Basic Constraints*
- *Key Usage*
- *Thumbprint algorithm*
- *Thumbprint*
- *Subject Alternative Names*
- *CRL Distribution Points*

7.1.2.1. Certificado Reconocido de Registrador

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1.17276.0.1.1.1		
Notice Referente	Certificado Reconocido de Registrador, sujeto a la DPC del CORPME, dirección prestador http://pki.registradores.org/normativa/direccion.html		
2. Subject Alternative Names	**Rfc6854Name** = correo_registrador@registradores.org **UPN** = UserID@Domain ➢ UPN OtherName OID es: "1.3.6.1.4.1.311.20.2.3" ➢ El valor "UPN OtherName" se debe codificar en UTF8 **1.3.6.1.4.1.17276.1.0.0.1**:Dirección Postal **1.3.6.1.4.1.17276.1.1.1.1**: Situación del Registrador	NO	[RFC6818]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc6854Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.

3. CRLDistributionPoints	**(1) HTTP:** http://pki.registradores.org/ /crls/crl_int_scr.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=CA%20INTERNA, OU=CERTIFICADO%20PROPIO, O=COLEGIO%20DE%20REGISTRADORES, C=ES ?certificateRevocationList?base ?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://ocsp.registradores.org/ **CA Raíz:** http://pki.registradores.org/ /certificados/ca_raiz_scr.crt	NO	

7.1.2.2. Certificado Reconocido de Personal Interno

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1.17276.0.1.2.1		
Notice Referente	Certificado Reconocido de Personal Interno, sujeto a la DPC del CORPME, dirección prestador http://pki.registradores.org/normativa/direccion.html		
2. Subject Alternative Names	**Rfc6854Name** = correo_registrador@registradores.org **UPN** = UserID@Domain ➢ UPN OtherName OID es: "1.3.6.1.4.1.311.20.2.3" ➢ El valor "UPN OtherName" se debe codificar en UTF8 **1.3.6.1.4.1.17276.1.0.0.1**:Dirección Postal **1.3.6.1.4.1.17276.1.1.2.1**: Subtipo **1.3.6.1.4.1.17276.1.1.2.2**: Sociedad	NO	[RFC6818]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc6854Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://pki.registradores.org/ /crls/crl_int_scr.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=CA%20INTERNA, OU=CERTIFICADO%20PROPIO, O=COLEGIO%20DE%20REGISTRADORES, C=ES ?certificateRevocationList?base ?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://ocsp.registradores.org/ **CA Raíz:** http://pki.registradores.org/ /certificados/ca_raiz_scr.crt	NO	

7.1.2.3. Certificado No Reconocido para Procedimientos Registrales

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1.17276.0.1.3.1		
Notice Referente	Certificado para Procedimientos Registrales, sujeto a la DPC del CORPME, dirección prestador http://pki.registradores.org/normativa/direccion.html		
2. Subject Alternative Names	**Rfc6854Name** = correo_registro@registradores.org **1.3.6.1.4.1.17276.1.0.0.1**:Dirección Postal	NO	[RFC6818]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc6854Name in the subject alternative name field (section 4.2.1.7) to describe such identities. Simultaneous inclusion of the EmailAddress attribute in the subject distinguished name to support legacy implementations is deprecated but permitted.
3. CRLDistributionPoints	**(1) HTTP:** http://pki.registradores.org/ /crls/crl_int_scr.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=CA%20INTERNA, OU=CERTIFICADO%20PROPIO, O=COLEGIO%20DE%20REGISTRADORES, C=ES ?certificateRevocationList?base ?objectclass=cRLDistributionPoint	NO	
4. Auth. Information	**OCSP:** http://ocsp.registradores.org/ **CA Raíz:** http://pki.registradores.org/ /certificados/ca_raiz_scr.crt	NO	

7.1.2.4. Certificado No Reconocido de Servidor de SSL

A continuación se presenta un detalle de las extensiones del certificado X.509 v3 más significativas:

Campo	Contenido Propuesto	Crítica	Observaciones
1. Certificate Policies	Se utilizará	NO	
Policy Identifier	1.3.6.1.4.1.17276.0.1.6.1		
Notice Referente	Certificado SSL, sujeto a la DPC del CORPME, dirección prestador		

	http://pki.registradores.org/normativa/direccion.html		
2. CRLDistributionPoints	**(1) HTTP:** http://pki.registradores.org/ /crls/crl_int_scr.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=CA%20INTERNA, OU=CERTIFICADO%20PROPIO, O=COLEGIO%20DE%20REGISTRADORES, C=ES ?certificateRevocationList?base ?objectclass=cRLDistributionPoint	NO	
3. Auth. Information	**OCSP:** http://ocsp.registradores.org/ **CA Raíz:** http://pki.registradores.org/ /certificados/ca_raiz_scr.crt	NO	

7.1.3. Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos: 1.3.6.1.4.1.17276.0.1.0.1.0

7.1.4. Formatos de nombres

Los certificados internos contienen el distinguished name X.500 del emisor y del titular del certificado en los campos *issuer name* y *subject* name respectivamente.

7.1.5. Restricciones de los nombres

Las restricciones de los nombres se encuentran descritas en el apartado 3.1.1 del presente documento.

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

Los OID para esta PC son los siguientes:

- Certificado Reconocido Registradores: 1.3.6.1.4.1.17276.0.1.1.1
- Certificados Reconocidos de Personal Interno: 1.3.6.1.4.1.17276.0.1.2.1
- Certificados no Reconocidos para Procedimientos Registrales: 1.3.6.1.4.1.17276.0.1.3.1
- Certificados no Reconocidos de servidores SSL: 1.3.6.1.4.1.17276.0.1.6.1

7.1.7. Uso de la extensión "PolicyConstraints"

No estipulado.

7.1.8. Sintaxis y semántica de los "PolicyQualifier"

El contenido de la extensión *Certificate Policies* puede consultarse en el apartado 7.1.2 del presente documento.

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

No estipulado.

7.2. PERFIL DE CRL

7.2.1. Número de versión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.2.2. CRL y extensiones

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.3. PERFIL DE OCSP

7.3.1. Número(s) de versión

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

7.3.2. Extensiones OCSP

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

8.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

8.5. ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

8.6. COMUNICACIÓN DE RESULTADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

9.1.1. Tarifas de emisión o renovación de certificado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.1.2. Tarifas de acceso a los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.1.4. Tarifas de otros servicios tales como información de políticas

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.1.5. Política de reembolso

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.2. RESPONSABILIDADES ECONÓMICAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.3.1. Ámbito de la información confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.3.2. Información no confidencial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.3.3. Deber de secreto profesional

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. Obligaciones de las CA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.6.2. Obligaciones de las RA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.6.3. Obligaciones de los titulares de los certificados

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.6.4. Obligaciones de los terceros que confían o aceptan los certificados del CORPME

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.6.5. Obligaciones de otros participantes

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.7. EXENCIÓN DE RESPONSABILIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.8. LIMITACIONES DE LAS RESPONSABILIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.9. INDEMNIZACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.10. PERÍODO DE VALIDEZ

9.10.1. Plazo

Esta PC entra en vigor desde el momento de su publicación en el directorio web del PSC del CORPME y se mantendrá vigente mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la Autoridad Certificadora de CORPME, momento en que obligatoriamente se dictará una nueva versión.

9.10.2. Sustitución y derogación de la PC

Esta PC será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la PC quede derogada se retirará del directorio web del PSC del CORPME, si bien se conservará durante quince (15) años.

9.10.3. Efectos de la finalización

Las obligaciones y restricciones que establece esta PC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades del PSC del CORPME, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.12. PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES

9.12.1. Procedimiento para los cambios

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.12.2. Circunstancias en las que el OID debe ser cambiado

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.13. RECLAMACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.14. NORMATIVA APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.16. ESTIPULACIONES DIVERSAS

9.16.1. Cláusula de aceptación completa

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.16.2. Independencia

En el caso de que una o más estipulaciones de esta PC sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la PC careciera ésta de toda eficacia.

9.16.3. Resolución por la vía judicial

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) del CORPME.

9.17. OTRAS ESTIPULACIONES

No estipulado.