Registradores DE ESPAÑA

POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS INTERNOS DEL CORPME

Prestador del Servicio de Certificación del Colegio de Registradores

Servicio de Sistemas de la Información

11 de noviembre de 2022

CONTROL DOCUMENTAL

DOCUMENTO / ARCHIVO	
Título: Políticas de Certificación de Certificados Internos del CORPME	Nombre Archivo/s: REG-PKI-DPC02v.3.0.5 Políticas de Certificación de Certificados Internos del CORPME.pdf
Código: REG-PKI-DPC02	Soporte lógico: MS-DOCX y PDF
Fecha: 11/11/2022	Ubicación física: http://pki.registradores.org/normativa/index.htm
Versión: 3.0.5	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
1.0.0	20/06/2016	Aprobación del documento
1.0.1	19/09/2016	Modificaciones LFE/2016/0071
1.0.2	27/10/2016	Modificaciones (2) LFE/2016/0071
1.0.3	23/11/2016	Modificaciones (3) LFE/2016/0071
1.0.4	23/12/2016	Modificaciones (4) LFE/2016/0071
1.0.5	29/05/2017	Adaptación al Reglamento eIDAS
1.1.0	26/06/2017	Adaptación debido a la auditoría de acuerdo a las normas ETSI
1.2.0	23/08/2017	Correcciones menores
1.3.0	25/05/2018	Adaptación al Reglamento General de Protección de Datos (UE) 2016/679 Especificación en certificado no cualificado de procedimientos registrales
1.4.0	16/06/2018	Especificación de casuísticas especiales en la generación de evidencias relativas a certificados cualificados de Registrador y de Personal Interno El campo UPN deja de ser opcional para los perfiles de Registrador y Personal Interno
2.0.0	01/04/2019	Inclusión de la fecha de revisión de la política de seguridad Restricción en los posibles solicitantes de los certificados Modificación de las fechas de validez de las evidencias Correcciones menores
3.0.0	01/06/2019	Modificación de los miembros de la autoridad de aprobación de políticas
3.0.1	24/02/2020	Ampliación del periodo de validez del certificado SSL de dos (2) a cinco (5) años.
3.0.2	12/03/2021	Adaptación a la nueva regulación de servicios de confianza
3.0.3	30/06/2021	Adaptación de plantillas de certificados a requisitos regulatorios
3.0.4	18/08/2021	Cambio en la jerarquía de la VA
3.0.5	11/11/2022	Especificaciones y requisitos para la emisión de certificados de cargos de Decanato. Cambio en la composición de la Comisión Directora del CORPME y alineamiento con la política de seguridad

ÍNDICE

1 INTRODUCCIÓN 8

1.1 VISIÓN GENERAL 8
1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 9
1.3 PARTICIPANTES EN LA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) DEL PRESTADOR DEL SERVICIO DE CERTIFICACIÓN DEL COLEGIO DE REGISTRADORES 9
1.3.1 Prestador de Servicios de Certificación (PSC) 9
1.3.2 Autoridad de Aprobación de Políticas 10
1.3.3 Autoridad de Certificación Raíz 11
1.3.4 Autoridades de Certificación Subordinadas 11
1.3.5 Autoridad de Registro 13
1.3.6 Autoridades de Validación (VA) 14
1.3.7 Autoridades de Sellado de Tiempo (TSA) 14
1.3.8 Entidades finales 14
1.4 USO DE LOS CERTIFICADOS 15
1.4.1 Usos adecuados de los certificados 15
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 las Políticas de Certificación 16
1.6 DATOS DE CONTACTO 17
1.7 DEFINICIONES Y ACRÓNIMOS 17
1.7.1 Definiciones 17
1.7.2 Acrónimos 20

2 DIRECTORIO Y PUBLICACIÓN DE INFORMACIÓN 22

2.1 DIRECTORIO DE VALIDACIÓN DE CERTIFICADOS 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 27
3.1.3 Reglas para interpretar varios formatos de nombres 27
3.1.4 Unicidad de los nombres 27
3.1.5 Procedimientos de resolución de conflictos sobre nombres 27
3.1.6 Reconocimiento, autenticación y papel de las marcas registradas 27
3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD 27
3.2.1 Medio de prueba de posesión de la clave privada 27
3.2.2 Autenticación de la identidad de una persona jurídica 28
3.2.3 Autenticación de la identidad de una persona física 28
3.2.4 Autenticación de la identidad de un dispositivo 31
3.2.5 Información no verificada sobre el solicitante 31
3.2.6 Comprobación de las facultades de representación 31
3.2.7 Criterios para operar con CA externas 31
3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN 31
3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN 32

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 33

4.1 SOLICITUD DE CERTIFICADOS 33
4.1.1 Quién puede efectuar una solicitud 33
4.1.2 Registro de las solicitudes de certificados y responsabilidades de los solicitantes 34
4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS 34
4.2.1 Realización de las funciones de identificación y autenticación 34
4.2.2 Aprobación o denegación de las solicitudes de certificados 34
4.2.3 Plazo para la tramitación de las solicitudes de certificados 34
4.3 EMISIÓN DE CERTIFICADOS 35
4.3.1 Actuaciones de la CA durante la emisión del certificado 35
4.3.2 Notificación al solicitante de la emisión por la CA del certificado 35
4.4 ACEPTACIÓN DEL CERTIFICADO 35
4.4.1 Mecanismo de aceptación del certificado 35
4.4.2 Publicación del certificado 35
4.4.3 Notificación de la emisión del certificado por la CA a otras Autoridades 35
4.5 PAR DE CLAVES Y USO DEL CERTIFICADO 35
4.5.1 Uso de la clave privada y del certificado por el titular 35
4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes 35
4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES 36
4.6.1 Circunstancias para la renovación de certificados sin cambio de claves 36
4.6.2 Quién puede solicitar la renovación de los certificados sin cambio de claves 36
4.6.3 Tramitación de las peticiones de renovación de certificados sin cambio de claves 36
4.6.4 Notificación de la renovación de un nuevo certificado al titular 36
4.6.5 Forma de aceptación del certificado sin cambio de claves 36
4.6.6 Publicación del certificado sin cambio de claves por la CA 36
4.6.7 Notificación de la renovación del certificado por la CA a otras Autoridades 36
4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES 36
4.7.1 Circunstancias para una renovación con cambio claves de un certificado 36
4.7.2 Quién puede solicitar la renovación de los certificados con cambio de claves 36
4.7.3 Tramitación de las peticiones de renovación de certificados con cambio de claves 37
4.7.4 Notificación de la renovación de un nuevo certificado al titular 37
4.7.5 Forma de aceptación del certificado con cambio de claves 37
4.7.6 Publicación del certificado con cambio de claves por la CA 37
4.7.7 Notificación de la renovación del certificado por la CA a otras Autoridades 37
4.8 MODIFICACIÓN DE CERTIFICADOS 37
4.8.1 Circunstancias para la modificación de un certificado 37
4.8.2 Quién puede solicitar la modificación de los certificados 37
4.8.3 Tramitación de las peticiones de modificación de certificados 37
4.8.4 Notificación de la modificación de un certificado al titular 37
4.8.5 Forma de aceptación del certificado modificado 37
4.8.6 Publicación del certificado modificado por la CA 37
4.8.7 Notificación de la modificación del certificado por la CA a otras Autoridades 38
4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS 38
4.9.1 Circunstancias para la revocación 38
4.9.2 Quién puede solicitar la revocación 38
4.9.3 Procedimiento de solicitud de revocación 38
4.9.4 Periodo de gracia de la solicitud de revocación 38
4.9.5 Plazo en el que la CA debe resolver la solicitud de revocación 38
4.9.6 Requisitos de verificación de las revocaciones por los terceros que confían 38
4.9.7 Frecuencia de emisión de CRL 38
4.9.8 Tiempo máximo entre la generación y la publicación de las CRL 38
4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados 38
4.9.10 Requisitos de comprobación en línea de revocación 39
4.9.11 Otras formas de divulgación de información de revocación disponibles 39
4.9.12 Requisitos especiales de revocación de claves comprometidas 39
4.9.13 Causas para la suspensión 39
4.9.14 Quién puede solicitar la suspensión 39

4.9.15 Procedimiento para la solicitud de suspensión ... 39
4.9.16 Límites del periodo de suspensión ... 39
4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS ... 39
4.10.1 Características operativas ... 39
4.10.2 Disponibilidad del servicio ... 39
4.10.3 Características adicionales ... 39
4.11 EXTINCIÓN DE LA VALIDEZ DE UN CERTIFICADO ... 40
4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES ... 40
4.12.1 Prácticas y políticas de custodia y recuperación de claves ... 40
4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión ... 40

5 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES ... 41

5.1 SEGURIDAD FÍSICA ... 41
5.1.1 Ubicación y medidas de seguridad física de las instalaciones de CORPME ... 41
5.1.2 Acceso físico ... 41
5.1.3 Suministro eléctrico y acondicionamiento ambiental de las instalaciones del CORPME ... 41
5.1.4 Exposición al agua ... 41
5.1.5 Medidas contra incendios e inundaciones. ... 41
5.1.6 Sistema de almacenamiento ... 41
5.1.7 Eliminación de residuos ... 41
5.1.8 Política de Respaldo de Información ... 41
5.2 CONTROLES DE PROCEDIMIENTO ... 41
5.2.1 Roles responsables del control y gestión de la PKI del CORPME ... 42
5.2.2 Número de personas requeridas por tarea ... 42
5.2.3 Roles que requieren segregación de funciones ... 42
5.3 CONTROLES DE PERSONAL ... 42
5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales ... 42
5.3.2 Procedimientos de comprobación de antecedentes ... 42
5.3.3 Requerimientos de formación ... 42
5.3.4 Requerimientos y frecuencia de actualización de la formación ... 42
5.3.5 Frecuencia y secuencia de rotación de tareas ... 42
5.3.6 Sanciones por actuaciones no autorizadas ... 42
5.3.7 Requisitos de contratación de terceros ... 42
5.3.8 Documentación proporcionada al personal ... 42
5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD ... 43
5.4.1 Tipos de eventos registrados ... 43
5.4.2 Frecuencia de procesado de registros de auditoría ... 43
5.4.3 Periodo de conservación de los registros de auditoría ... 43
5.4.4 Protección de los registros de auditoría ... 43
5.4.5 Procedimientos de respaldo de los registros de auditoría ... 43
5.4.6 Notificación al sujeto causa del evento ... 43
5.4.7 Análisis de vulnerabilidades ... 43
5.5 ARCHIVADO DE REGISTROS ... 43
5.5.1 Tipo de eventos archivados ... 43
5.5.2 Periodo de conservación de registros ... 43
5.5.3 Protección del archivo ... 43
5.5.4 Procedimientos de copia de respaldo del archivo ... 44
5.5.5 Requerimientos para el sellado de tiempo de los registros ... 44
5.5.6 Sistema de archivo de información (interno vs externo) ... 44
5.5.7 Procedimientos para obtener y verificar información archivada ... 44
5.6 CAMBIO DE CLAVES ... 44
5.7 RECUPERACIÓN ANTE COMPROMISO DE CLAVE O CATÁSTROFE ... 44
5.7.1 Procedimientos de gestión de incidentes y compromisos ... 44
5.7.2 Alteración de los recursos hardware, software y/o datos ... 44
5.7.3 Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad ... 44
5.7.4 Instalación después de un desastre natural u otro tipo de catástrofe ... 44

5.8 CESE DE UNA CA O RA 44
5.8.1 Cese de una CA 45
5.8.2 Cese de una RA 45

6 CONTROLES DE SEGURIDAD TÉCNICA 46

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 46
6.1.1 Generación del par de claves 46
6.1.2 Entrega de la clave privada al titular 46
6.1.3 Entrega de la clave pública al emisor del certificado 46
6.1.4 Entrega de la clave pública de la CA a los terceros que confían 46
6.1.5 Tamaño de las claves 46
6.1.6 Parámetros de generación de la clave pública y verificación de la calidad 46
6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3) 46
6.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS 47
6.2.1 Estándares para los módulos criptográficos 47
6.2.2 Control multipersona (k de n) de la clave privada 47
6.2.3 Custodia de la clave privada 47
6.2.4 Copia de seguridad de la clave privada 47
6.2.5 Archivado de la clave privada 47
6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico 47
6.2.7 Almacenamiento de la clave privada en un módulo criptográfico 47
6.2.8 Método de activación de la clave privada 47
6.2.9 Método de desactivación de la clave privada 47
6.2.10 Método de destrucción de la clave privada 48
6.2.11 Clasificación de los módulos criptográficos 48
6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 48
6.3.1 Archivo de la clave pública 48
6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves 48
6.4 DATOS DE ACTIVACIÓN 48
6.4.1 Generación e instalación de los datos de activación 48
6.4.2 Protección de los datos de activación 48
6.4.3 Otros aspectos de los datos de activación 48
6.5 CONTROLES DE SEGURIDAD INFORMÁTICA 48
6.5.1 Requerimientos técnicos de seguridad específicos 48
6.5.2 Evaluación de la seguridad informática 48
6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 49
6.6.1 Controles de desarrollo de sistemas 49
6.6.2 Controles de gestión de seguridad 49
6.6.3 Controles de seguridad del ciclo de vida 49
6.7 CONTROLES DE SEGURIDAD DE LA RED 49
6.8 SELLADO DE TIEMPO 49

7 PERFILES DE LOS CERTIFICADOS, CRL Y OCSP 50

7.1 PERFIL DE CERTIFICADO 50
7.1.1 Número de versión 50
7.1.2 Extensiones del certificado 50
7.1.3 Identificadores de objeto (OID) de los algoritmos 60
7.1.4 Formatos de nombres 60
7.1.5 Restricciones de los nombres 60
7.1.6 Identificador de objeto (OID) de la Política de Certificación 60
7.1.7 Uso de la extensión "PolicyConstraints" 61
7.1.8 Sintaxis y semántica de los "PolicyQualifier" 61
7.1.9 Tratamiento semántico para la extensión crítica "Certificate Policy" 61
7.2 PERFIL DE CRL 61
7.2.1 Número de versión 61
7.2.2 CRL y extensiones 61

7.3 PERFIL DE OCSP 61
7.3.1 Número(s) de versión 61
7.3.2 Extensiones OCSP 61

8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES 62

8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD 62
8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR 62
8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA 62
8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES 62
8.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS 62
8.6 COMUNICACIÓN DE RESULTADOS 62

9 OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD 63

9.1 TARIFAS 63
9.1.1 Tarifas de emisión o renovación de certificado 63
9.1.2 Tarifas de acceso a los certificados 63
9.1.3 Tarifas de acceso a la información de estado o revocación 63
9.1.4 Tarifas de otros servicios tales como información de políticas 63
9.1.5 Política de reembolso 63
9.2 RESPONSABILIDADES ECONÓMICAS 63
9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN 63
9.3.1 Ámbito de la información confidencial 63
9.3.2 Información no confidencial 63
9.3.3 Deber de secreto profesional 63
9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL 64
9.5 DERECHOS DE PROPIEDAD INTELECTUAL 64
9.6 REPRESENTACIONES Y GARANTÍAS 64
9.6.1 Obligaciones de las CA's 64
9.6.2 Obligaciones de las RA's 64
9.6.3 Obligaciones de los titulares de los certificados 64
9.6.4 Obligaciones de los terceros que confían o aceptan los certificados del CORPME 64
9.6.5 Obligaciones de otros participantes 64
9.7 EXENCIÓN DE RESPONSABILIDADES 64
9.8 LIMITACIONES DE LAS RESPONSABILIDADES 64
9.9 INDEMNIZACIONES 64
9.10 PERÍODO DE VALIDEZ 64
9.10.1 Plazo 64
9.10.2 Sustitución y derogación de la PC 65
9.10.3 Efectos de la finalización 65
9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES 65
9.12 PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES 65
9.12.1 Procedimiento para los cambios 65
9.12.2 Circunstancias en las que el OID debe ser cambiado 65
9.13 RECLAMACIONES 65
9.14 NORMATIVA APLICABLE 65
9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE 65
9.16 ESTIPULACIONES DIVERSAS 66
9.16.1 Cláusula de aceptación completa 66
9.16.2 Independencia 66
9.16.3 Resolución por la vía judicial 66
9.17 OTRAS ESTIPULACIONES 66

1 INTRODUCCIÓN

1.1 Visión general

El Colegio de Registradores de la Propiedad y Mercantiles 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 la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, 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. Los estándares y normativas que se aplican y cumplen con el presente documento son:

- **RFC 3647**: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*
- **RFC 3739:** *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.*
- **ETSI EN 319 401***: General Policy Requirements for Trust Service Providers.*
- **ETSI EN 319 411-1***: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.*
- **ETSI EN 319 411-2***: Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates.*
- **ETSI EN 319 412-1***: Certificate Profiles. Overview and common data structures.*
- **ETSI EN 319 412-2***: Certificate Profiles. Certificate profile for certificates issued to natural persons.*
- **ETSI EN 319 412-3***: Certificate Profiles. Certificate profile for certificates issued to legal persons.*
- **ETSI EN 319 412-5***: Certificate Profiles. QCStatements.*
- **CA/Browser Forum:** *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.*

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 DPC 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.

Los certificados cualificados incluidos en las respectivas PC's, cumplen con la normativa de certificados "EU Qualified" y requieren el uso de un Dispositivo Seguro de Creación de Firma.

La actividad del CORPME se desarrollará con plena sujeción a las prescripciones de la Ley 24/2001, de 27 de diciembre, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, de 20 de diciembre, todas de ámbito estatal; al reglamento EU 910/2014 de Identificación electrónica y de servicios de confianza, 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

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

Identificación del Documento:

Nombre del documento	Políticas de Certificación de Certificados Internos del CORPME
Versión del documento	3.0.5
Estado del documento	Versión
Fecha de emisión	11/11/2022
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.1.0.3.0.2
Ubicación de la PC	http://pki.registradores.org/normativa/index.htm
DPC Relacionada	Declaración de Prácticas de Certificación

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.

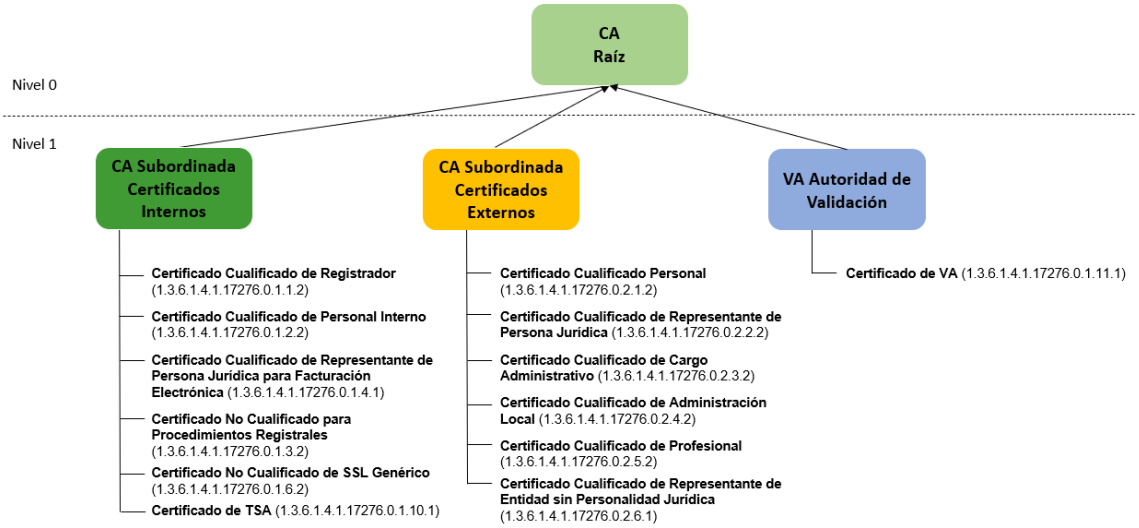
La información legal y datos identificativos del Prestador de Servicios de Certificación del CORPME estarán siempre disponibles en http://pki.registradores.org/normativa/index.htm. También podrá solicitarse una copia impresa de dicha documentación previa solicitud del interesado en la dirección siguiente:

Colegio de Registradores de la Propiedad y Mercantiles 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 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el reglamento EU 910/2014 de identificación electrónica y de servicios de confianza.

Los servicios de certificación se aplican, en cualquier caso, con arreglo al principio de no discriminación.

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 PC's 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, que está definido de manera formal en la Política de Seguridad de la Información y Privacidad, constituida por los siguientes vocales:

- El Vocal de Relaciones Institucionales del Colegio de Registradores, que actuará como Presidente del Comité y que en caso de empate en una votación tendrá voto de calidad.
- El Vicedecano del Colegio de Registradores.
- El Vocal Secretario del Colegio de Registradores.
- El Vocal del Servicio de Sistemas de Información del Colegio de Registradores, que actuará como Secretario del Comité.
- El Vocal de Responsabilidad Social Corporativa
- El Vocal del Servicio de Oficinas Liquidadoras e Innovación.

El nombramiento y renovación de sus miembros se realizará de acuerdo con lo regulado para los cargos que los mismos llevan asociados.

Asimismo, los miembros de Comisión Directora pueden disponer de roles de apoyo los cuales forman parte de esta Comisión y su rol consiste en asesorar a este órgano de gobierno en las materias que les competen, pudiendo proponer decisiones a tomar, si bien no disponen de voto efectivo.

En el ámbito de la actividad de la AAP se implementarán mecanismos de quorum que garanticen el consenso sobre las decisiones que se tomen potenciando la flexibilidad en la disponibilidad de los distintos miembros que componen la AAP. En este sentido el quorum mínimo será de dos (2) miembros de la AAP garantizando, en cualquier caso, que el Vocal del Servicio de Sistemas de Información y el Vocal del Servicio de Oficinas Liquidadoras e Innovación son partícipes de la toma de decisiones relativa a las prácticas del PSC.

Se implementa un proceso de aprobación ágil que no requiera una convocatoria formal de reunión de los miembros de la AAP sino un proceso de validación consensuada mediante métodos de comunicación ágiles. Las decisiones que se tomen utilizando el método de aprobación ágil serán consolidadas en la primera convocatoria de la AAP inmediatamente posterior a la toma de decisión ágil.

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 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 = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Número de serie	3b 38 d3 bf 57 b2 94 43 57 55 5d 78 9c fd 5e 5f
Nombre distintivo del emisor	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Fecha de emisión	lunes, 06 de junio de 2016 13:24:40
Fecha de expiración	miércoles, 06 de junio de 2040 13:24:40
Longitud de clave RSA	4096 Bits
Algoritmo hash de firma	SHA-512
Huella digital (SHA-1)	97 4e 26 df 10 d2 c2 00 24 b2 1c 4a 0e b9 c7 ef 5c 06 80 d4
URL de publicación del certificado	http://pki.registradores.org/certificados/ac_raiz_psc_corpme.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 = Autoridad de Certificación de los Registradores - AC Interna, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Número de serie	19 03 bc e3 42 82 77 60 57 55 8a f9 e9 b7 7e 2b
Nombre distintivo del emisor	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Fecha de emisión	lunes, 06 de junio de 2016 16:38:48
Fecha de expiración	martes, 06 de junio de 2028 16:38:48
Longitud de clave RSA	4096 Bits
Algoritmo hash de firma	SHA-512
Huella digital (SHA-1)	11 bb d7 b4 a3 08 05 6e 15 13 20 1e 36 b6 9e a9 4e a9 f2 f9
URL de publicación del certificado	http://pki.registradores.org/certificados/ac_int_psc_corpme.crt
URL de publicación de la CRL	http://pki.registradores.org/crls/crl_int_psc_corpme.crl
Tipos de certificados emitidos	**Certificado Cualificado de Registrador** (1.3.6.1.4.1.17276.0.1.1.2): el suscriptor representa una persona natural asociada a una persona legal. **Certificado Cualificado de Personal Interno** (1.3.6.1.4.1.17276.0.1.2.2): el suscriptor representa una persona natural asociada a una persona legal. **Certificado Cualificado de Representante de Persona Jurídica para Facturación Electrónica** (1.3.6.1.4.1.17276.0.1.4.1): el suscriptor representa una persona natural asociada a una persona legal, representando a esta persona legal. **Certificado No Cualificado para Procedimientos Registrales** (1.3.6.1.4.1.17276.0.1.3.2). **Certificado No Cualificado de SSL Genérico** (1.3.6.1.4.1.17276.0.1.6.2). **Certificado de TSA** (1.3.6.1.4.1.17276.0.1.10.1). **Certificado de VA** (1.3.6.1.4.1.17276.0.1.11.1).

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

Nombre distintivo	CN = Autoridad de Certificación de los Registradores - AC Externa, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Número de serie	0f 58 42 bf f2 91 93 45 57 55 91 64 34 56 36 54
Nombre distintivo del emisor	CN = Autoridad de Certificación Raíz de los Registradores, O = Colegio de Registradores de la Propiedad y Mercantiles, 2.5.4.97 = VATES-Q2863012G, C = ES
Fecha de emisión	lunes, 06 de junio de 2016 17:06:11
Fecha de expiración	martes, 06 de junio de 2028 17:06:11

Longitud de clave RSA	4096 Bits
Algoritmo hash de firma	SHA-512
Huella digital (SHA-1)	e1 37 72 e5 a9 d6 2f 3f 5a 0a b1 ad ec 80 51 68 75 96 fb 70
URL de publicación del certificado	http://pki.registradores.org/certificados/ac_ext_psc_corpme.crt
URL de publicación de la CRL	http://pki.registradores.org/crls/crl_ext_psc_corpme.crl
Tipos de certificados emitidos	**Certificado Cualificado Personal** (1.3.6.1.4.1.17276.0.2.1.2): el suscriptor representa una persona natural. **Certificado Cualificado de Representante de Persona Jurídica** (1.3.6.1.4.1.17276.0.2.2.2): el suscriptor representa una persona natural asociada a una persona legal, representando a esta persona legal. **Certificado Cualificado de Cargo Administrativo** (1.3.6.1.4.1.17276.0.2.3.2): el suscriptor representa una persona natural asociada a una persona legal. **Certificado Cualificado de Administración Local** (1.3.6.1.4.1.17276.0.2.4.2): el suscriptor representa una persona natural asociada a una persona legal. **Certificado Cualificado de Profesional** (1.3.6.1.4.1.17276.0.2.5.2): el suscriptor representa una persona natural. **Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica** (1.3.6.1.4.1.17276.0.2.6.1): el suscriptor representa una persona natural asociada a una entidad organizativa que no es una persona legal, representando a esta entidad.

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, interino 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 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://pki.registradores.org/agenda**, en una única comparecencia, el día y hora de su elección en la Unidad de Tramitación.

1.3.6 Autoridades 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 Autoridades 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.

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 o entidad sin personalidad 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://pki.registradores.org/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 la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y del reglamento EU 910/2014, 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.

Igualmente, tendrá la consideración de Suscriptor a los efectos de la Ley de Firma Electrónica y del reglamento EU 910/2014 la persona física indicada en los siguientes casos:

- En caso de la emisión de Certificados de Representante de Persona Jurídica, 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.
- En caso de la emisión de Certificados de Representante de Entidad sin Personalidad Jurídica, la persona física, en virtud del nombramiento publicado en el Boletín Oficial del Estado, incluyéndose los datos de éste en el certificado.
- En el caso de aquellos perfiles específicos de certificados de Representantes de Entidad Jurídicas emitidos a personas físicas, la persona física solicitante que acreditará su capacidad para su solicitud y tramitación en la Unidad de Tramitación Central.

La identidad del Suscriptor en tanto que titular del certificado figurará en el campo *Distinguished Name* del certificado digital, en los atributos *CN (Common Name),* SN *(Serial Number),* G *(Given Name*) y S (*Surname*), dentro del campo *Subject* del certificado. Los datos identificativos del Suscriptor podrán ser así mismo incluidos, dependiendo del tipo de certificado, en una extensión de nombre alternativo *subjectAltName*, de conformidad con lo que se estipule en las políticas particulares aplicables a cada certificado.

En los casos de la representación de Personas Jurídicas o de Entidades sin Personalidad Jurídica, los datos de la representación quedarán reflejados en el atributo *Description* del campo *Distinguished Name* del certificado digital.

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, la Administración General del Estado y otro tipo de Organismos y Entidades, 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 Servicio de Sistemas de Información (en adelante, 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 DPC 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 Director del PSC promoverá convocar el Comité Técnico de Asesoramiento y Cumplimiento Normativo para trasladar cambios en la DPC y las PC's del PSC del CORPME o será convocado por el propio Comité.

El Comité técnico de Asesoramiento y Cumplimiento Normativo realizará, al menos, una revisión anual de dichos documentos.

1.5.2 Procedimiento de aprobación y modificación de las Políticas de Certificación

La aprobación y subsiguientes modificaciones de la 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 DPC el interesado deberá dirigirse al CORPME a través de alguno de los siguientes medios:

Colegio de Registradores de la Propiedad y Mercantiles de España
Prestador de Servicios de Certificación del Colegio de Registradores
C/ DIEGO DE LEON, 21
28006-MADRID
Email: psc@registradores.org
Telf.: 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 PC, 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 cualificado: 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 del 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 (DSCF): 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.

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 cualificada: Es aquella Firma Electrónica avanzada basada en un certificado cualificado y generada mediante un DSCF.

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.

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 PC, se corresponderá con las Autoridades de Certificación pertenecientes a la jerarquía de CORPME.

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

Póliza: A efectos de la presente PC 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. Se utiliza para desbloquear el acceso a dicho recurso.

RGPD (Reglamento General de Protección de Datos): Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

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.

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 DSCF de acuerdo con la Ley y permite la generación de Firma Electrónica cualificada.

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 la DPC.

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.

CORPME: Colegio de Registradores de la Propiedad y Mercantiles 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.

DPC: Declaración de Prácticas de Certificación (Certification Practice Statement).

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).

PSC: Proveedor de Servicios de Certificación.

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: Time Stamping Authority (Autoridad de Sellado de Tiempo).

TST: Time Stamp Token (Token de Sellado de Tiempo).

TSU: Time Stamping Unit (Unidad de Sellado de Tiempo).

UTC: Universal Time Coordinated.

VA: Validation Authority (Autoridad de Validación).

2 DIRECTORIO 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 del 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_psc_corpme.crl
CRL CA Certificados Internos	http://pki.registradores.org/crls/crl_int_psc_corpme.crl
CRL CA Certificados Externos	http://pki.registradores.org/crls/crl_ext_psc_corpme.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/ac_raiz_psc_corpme.crt
Certificado CA Internos	http://pki.registradores.org/certificados/ac_int_psc_corpme.crt
Certificado CA Externos	http://pki.registradores.org/certificados/ac_ext_psc_corpme.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 PC's 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 PC's 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 Cualificado de Registrador

La estructura del certificado, referente al campo *Subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-Q2863012G	NIF (Requerido por ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organización.
OU	*NOMBRE REGISTRO*	Registro en el que ejerce su función el titular del certificado. Todos los datos deben ir en MAYÚSCULAS.
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Requerido por ETSI EN 319 412-2.
SN	*APELLIDOS*	**surname.** Requerido por ETSI EN 319 412-2. Todos los datos deben ir en MAYÚSCULAS.
G	*NOMBRE*	**givenName.** Requerido por ETSI EN 319 412-2. Todos los datos deben ir en MAYÚSCULAS.
CN	NOMBRE *NOMBRE APELLIDOS* – NIF *NIF*	Todos los datos deben ir en MAYÚSCULAS.

3.1.1.2 Certificado Cualificado de Personal Interno

La estructura del certificado, referente al campo *Subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-Q2863012G	NIF (Requerido por ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organización.
OU	*NOMBRE REGISTRO O UNIDAD DESTINO*	Todos los datos deben ir en MAYÚSCULAS.
SERIALNUMBER	IDCES-*NIF*	**serialNumber.** Requerido por ETSI EN 319 412-2.
SN	*APELLIDOS*	**surname.** Requerido por ETSI EN 319 412-2. Todos los datos deben ir en MAYÚSCULAS.
G	*NOMBRE*	**givenName.** Requerido por ETSI EN 319 412-2. Todos los datos deben ir en MAYÚSCULAS.
CN	NOMBRE *NOMBRE APELLIDOS* – NIF *NIF*	Todos los datos deben ir en MAYÚSCULAS.

3.1.1.3 Certificado Cualificado de Representante de Persona Jurídica para Facturación Electrónica

La estructura del certificado, referente al campo *Subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País.
description	Reg: Registro salida CORPME /Fecha: *DD-MM-AAAA* /Numero: *NUM*	Codificación del documento oficial que acredita las facultades del firmante y su registro en el fichero del Colegio de Registradores.
organizationIdentifier	VATES-*NIF*	NIF de la entidad (@firma y requerido por ETSI 319 412-2).
O	*RAZÓN SOCIAL*	Organización para @firma (Requerido por ETSI 319 412-2). Todos los datos deben ir en MAYÚSCULAS.

SERIALNUMBER	IDCES-*DNI / NIE / PASAPORTE*	**serialNumber.** Requerido por ETSI EN 319 412-2.
SN	*APELLIDOS*	**surname.** Requerido por ETSI EN 319 412-2. Todos los datos deben ir en MAYÚSCULAS.
G	*NOMBRE*	**givenName.** Requerido por ETSI EN 319 412-2. Todos los datos deben ir en MAYÚSCULAS.
CN	*DNI NOMBRE APELLIDOS* (R: *NIF*)	Todos los datos deben ir en MAYÚSCULAS. El campo tiene un tamaño máximo de 64 caracteres según la RFC 5280.

3.1.1.4 Certificado No Cualificado para Procedimientos Registrales

La estructura del certificado, referente al campo *Subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-Q2863012G	NIF (Requerido por ETSI 319 412-2).
O	Colegio de Registradores de la Propiedad y Mercantiles	Organización.
CN	*NOMBRE REGISTRO o* *SERVICIO DE SISTEMAS DE INFORMACIÓN*	Registro titular del certificado o Servicio de Sistemas de Información. Todos los datos deben ir en MAYÚSCULAS.

3.1.1.5 Certificado No Cualificado de SSL Genérico

La estructura del certificado, referente al campo *Subject* del certificado, es la que se describe en la siguiente tabla:

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-Q2863012G	NIF (Requerido por ETSI 319 412-2).

O	Colegio de Registradores de la Propiedad y Mercantiles	Organización.
CN	*<Nombre Máquina / Nombre DNS>*	

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 Cualificados 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 Cualificados de Personal Interno, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF en el CN garantiza la unicidad del mismo.
- Para Certificado No Cualificado de Procedimientos Registrales, el uso del nombre del registro titular del certificado o Servicio de Sistemas de información en el CN, garantiza la unicidad del mismo.
- Para Certificado No Cualificado de SSL Genérico, el uso del nombre de máquina en el CN, garantiza la unicidad del mismo.
- Para los Certificados Cualificados de Representante de Persona Jurídica para Facturación Electrónica, el uso de la entidad (compuesto por la razón social), del NIF, del nombre (compuesto por los apellidos y el nombre), y del NIF 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 privadas de los certificados internos:

- Certificado Cualificado de Registrador
- Certificado Cualificado de Personal Interno
- Certificado Cualificado de Representante de Persona Jurídica para Facturación Electrónica

Serán generadas por el dispositivo criptográfico seguro del solicitante estando bajo la custodia de éste. Dentro del dispositivo, se llevarán a cabo tanto la generación de claves como las operaciones criptográficas de firma, de manera directa e inmediata. De este modo, en ningún caso será necesario transferir a un equipo externo la clave privada, garantizando así al suscriptor su absoluto control sobre los datos de creación de firma, y, por ende, la imposibilidad de suplantación de su firma electrónica. La orden de generación de las claves y la introducción de las contraseñas del dispositivo criptográfico serán realizadas personalmente por el titular del certificado.

Para los Certificados No Cualificados de SSL Genérico 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 Cualificados 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.

Siendo necesario para garantizar la continuidad de los servicios registrales, el CORPME con la asistencia de la UT Central podrá emitir de oficio el Certificado No Cualificado para Procedimientos Registrales, sin perjuicio de las responsabilidades que eso conlleve para el Registro en cuestión. Si emitido el certificado y a falta que transcurran 7 días hábiles, no se ha iniciado el proceso de instalación por parte del registro, la Unidad de Tramitación Central y los servicios técnicos del CORPME podrán iniciarla en aquellos elementos que sean críticos para el mantenimiento de la prestación del servicio público del registro. Esta situación será regularizada mediante las debidas actuaciones que garanticen el reconocimiento de las responsabilidades por parte de los responsables del Registro.

3.2.2 Autenticación de la identidad de una persona jurídica

Los solicitantes nacionales de Certificados del CORPME, deberán comparecer ante la Unidad de Tramitación de su elección, provistos de su NIF.

Los solicitantes extranjeros de Certificados del CORPME, deberán comparecer, provistos de su número de identificación de extranjeros (NIE) y de su pasaporte, de su tarjeta de residencia o cualquier otro documento legal de identificación que disponga de una imagen del rostro del solicitante.

Además de la identificación del solicitante como persona física, mediante la comprobación de la documentación señalada anteriormente, el Responsable de la Unidad de Tramitación correspondiente solicitará la documentación acreditativa del atributo certificable de que se trate en virtud del tipo de certificado.

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 Cualificado de Registrador

- Nombre del registro (registro en el que ejerce su función el titular del certificado).
- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF) del suscriptor.

- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Nombre Principal de Windows (UPN).
- Cargo.
  - Registrador Activo.
    - Certificado expedido de manera online o registro electrónico que confirma el cargo correspondiente.

3.2.3.2 Certificado Cualificado de Personal Interno

- Nombre del Registro o de la Unidad Destino.
  - En el caso de empleados de Registro: Registro en el que ejerce su función el titular del certificado.
  - En el caso de cargos de Decanato o empleados del Decanato: Decanato en el que ejerce su función el titular del certificado.
  - En el caso de empleados del Colegio de Registradores, cargos del Colegio de Registradores, cargos de la Junta de Gobierno del Colegio de Registradores, Registradores aspirantes, Registradores jubilados, Registradores excedentes y empleados de sociedades colegiales, personal de organizaciones externas que dan servicio al CORPME..
- Nombre y apellidos del suscriptor.
- Documento identificativo del suscriptor.
  - En el caso de cargos de la Junta de Gobierno del Colegio de Registradores, Registradores aspirantes, Registradores jubilados, Registradores excedentes: DNI/NIF.
  - En el caso de empleados del Colegio de Registradores, empleados de Registro, empleados de Decanato, cargos del Colegio de Registradores y empleados de sociedades colegiales, personal de organizaciones externas que dan servicio al CORPME: DNI/NIF o NIE, en cuyo caso deberá aportar, además, su pasaporte, su tarjeta de residencia o cualquier otro documento legal de identificación que disponga de una imagen del rostro del solicitante.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Nombre Principal de Windows (UPN).
- Subtipo: Colegio, Registro, Organización (sociedades colegiales), Decanato, Registrador aspirante, Registrador jubilado, Registrador excedente, Personal de organizaciones externas que dan servicio al CORPME.
- Denominación de la Organización (si aplica).
- Cargo.
  - Empleado del Colegio de Registradores.
    - Declaración responsable expedida por el Vicedecano o Director de Recursos Humanos del Colegio de Registradores, o por quien éste haya delegado, que confirme el cargo correspondiente.
  - Empleado de Registro de la Propiedad o Mercantil.

        - Declaración responsable expedida por el Registrador que confirme el cargo correspondiente.
    - Cargo del Decanato
        - Declaración responsable expedida por el Secretario del Decanato que confirme el cargo correspondiente. En el caso del cargo de Secretario, la declaración responsable será expedida por el Decano.
    - Empleado del Decanato
        - Declaración responsable expedida por el Decano que confirme el cargo.
    - Cargo del Colegio de Registradores.
        - Declaración responsable expedida por el Vicedecano o Director de Recursos Humanos del Colegio de Registradores, o por quien éste haya delegado, que confirme el cargo correspondiente.
    - Cargo de la Junta de Gobierno del Colegio de Registradores.
        - Declaración responsable expedida por el Secretario del Colegio de Registradores que confirme el cargo correspondiente. En el caso del cargo de Secretario, la declaración responsable será expedida por el Decano-Presidente del Colegio de Registradores
    - Registrador aspirante.
        - Certificado expedido de manera online o por la Secretaría del Colegio de Registradores que confirma el cargo correspondiente.
    - Registrador jubilado.
        - Certificado expedido de manera online o por la Secretaría del Colegio de Registradores que confirma el cargo correspondiente.
    - Registrador excedente.
        - Certificado expedido de manera online o por la Secretaría del Colegio de Registradores que confirma el cargo correspondiente.
    - Personal de organizaciones externas que dan servicio al CORPME.
        - Certificado de la organización externa donde conste la identidad del personal y su asignación al servicio prestado para el PSC. Este certificado será aportado por el Director Financiero del SSI del CORPME, como responsable de los contratos con terceros.

3.2.3.3 Certificado Cualificado de Representante de Persona Jurídica para Facturación electrónica

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF) del suscriptor.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Razón Social.
- NIF del Colegio de Registradores.
- Cargo.
    - Decano-Presidente del Colegio de Registradores.

- Declaración responsable expedida por el Secretario del Colegio de Registradores que confirma el cargo correspondiente, y
- Copia del registro de salida del Colegio de Registradores con la notificación oficial al Director General de los Registros y del Notariado del nombramiento del Decano-Presidente.

- Número de salida.
- Fecha de salida del documento.

3.2.3.4 Autenticación de la identidad de un dispositivoCertificado No Cualificado para Procedimientos Registrales

- Nombre del registro titular del certificado.
- Correo electrónico (opcional).
- Dirección postal.
- Operador.

3.2.3.5 Certificado No Cualificado de SSL Genérico

- Nombres de la Máquina o Nombres DNS.
- Correo electrónico.

3.2.4 Información no verificada sobre el solicitante

Toda la información presentada por el solicitante es verificada antes de la emisión del certificado que solicita.

3.2.5 Comprobación de las facultades de representación

Además de la identificación del solicitante como persona física, mediante la comprobación de la documentación señalada anteriormente, el Responsable de la Unidad de Tramitación correspondiente solicitará la documentación acreditativa del atributo certificable de que se trate en virtud del tipo de certificado.

La Unidad de Tramitación comprobará la equivalencia de la certificación con los términos en los que queda redactado el certificado, así como la exacta correlación entre los periodos de vigencia del atributo inscrito y del certificado. Si se detecta alguna inexactitud procederá a revocar el certificado dentro de este plazo, notificando este hecho al titular.

3.2.6 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.

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.

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 cualificado solicitado.

Para la solicitud de algunos de los certificados emitidos por el CORPME se puede requerir la petición de cita previa.

4.1.1.1 Certificado Cualificado de Registrador

La solicitud de este tipo de certificados se podrá efectuar por parte de los Registradores en activo.

El proceso de solicitud no requiere de cita previa. La solicitud se llevará a cabo mediante la creación de una cita falsa para solicitar y validar los datos del usuario y proceder a la invocación de la emisión del certificado.

Los usuarios que soliciten este tipo de certificados, se personarán con documento identificativo correspondiente y una certificación que acredite el cargo.

4.1.1.2 Certificado Cualificado de Personal Interno

La solicitud de este tipo de certificados se podrá efectuar por parte de los empleados del Colegio de Registradores, empleados de Registro, cargos de los Decanatos, empleados del Decanato, cargos del Colegio de Registradores, cargos de la Junta de Gobierno del Colegio de Registradores, Registradores aspirantes, Registradores jubilados, Registradores excedentes y empleados de sociedades colegiales, personal de organizaciones externas que dan servicio al CORPME.

El proceso de solicitud no requiere de cita previa. La solicitud se llevará a cabo mediante la creación de una cita falsa para solicitar y validar los datos del usuario y proceder a la invocación de la emisión del certificado.

Los usuarios que soliciten este tipo de certificados, se personarán con documento identificativo correspondiente y una certificación que acredite el cargo.

4.1.1.3 Certificado Cualificado de Representante de Persona Jurídica para Facturación Electrónica

La solicitud de este tipo de certificados se podrá efectuar por parte del Decano-Presidente del Colegio de Registradores.

El proceso de solicitud no requiere de cita previa. La solicitud se llevará a cabo mediante la creación de una cita falsa para solicitar y validar los datos del usuario y proceder a la invocación de la emisión del certificado.

Los usuarios que soliciten este tipo de certificados, se personarán con documento identificativo correspondiente y una certificación que acredite el cargo.

4.1.1.4 Certificado No Cualificado para Procedimientos Registrales

Los Certificados No Cualificados 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.

4.1.1.5 Certificado No Cualificado de SSL Genérico

Para la emisión de Certificados No Cualificados de SSL Genérico 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

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

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

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

El solicitante deberá firmar la licencia de uso del certificado, aceptando el mismo y la presente PC. La licencia incluirá necesariamente los siguientes contenidos:

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

4.5.2 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 renovación 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 renovación del certificado por la CA a otras Autoridades

No estipulado.

4.7 Renovación de certificados con cambio de claves

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

4.7.1 Circunstancias para una renovación con cambio claves de un certificado

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

4.7.2 Quién puede solicitar la renovación de los certificados con cambio de claves

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 renovación 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 cambio de claves

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

4.7.6 Publicación del certificado con cambio de claves por la CA

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

4.7.7 Notificación de la renovación 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

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

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 modificación de un certificado 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

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

4.9.3 Procedimiento de solicitud de revocación

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

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 FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

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 Notificación al sujeto causa del evento

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

5.4.7 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 (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 Cese de una CA

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

5.8.2 Cese de una RA

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 2048 bits para todos los certificados.

Para los certificados cualificados (Registradores, Personal Interno, y Representante de Persona Jurídica para Facturación Electrónica) son generadas siempre durante la comparecencia del solicitante y con su intervención personal en el proceso de asignación de claves.

Para los certificados no cualificados (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's 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 la CA de Certificados Internos es de 4096 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 RFC 5280 y RFC 3279.

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 internos 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's 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 Archivado 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, así como los certificados de procedimientos registrales cuya duración será de (3) 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 en los certificados son:

- *Subject Key Identifier*
- *Authority Key Identifier*
- *Certificate Policies*
- *Basic Constraints*
- *Key Usage*
- *Extended Key Usage*
- *Subject Alternative Name*
- *CRL Distribution Points*
- *Authority Information Access (AIA)*
- *Extensiones de certificado cualificado EU (EU-qualified)*
    - *Qualified Certificate Statements*
    - *QCSyntax v2*
    - *EU Qualified Certificate Policy Identifier*

7.1.2.1 Certificado Cualificado de Registrador

A continuación, se presentan los campos y extensiones del certificado X.509 v3:

Campo / Extensión	Contenido	Crítica	Observaciones
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.

Validity	2 años		
Subject	Como está definido en el apartado 3.1.1.1		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. El atributo *SerialNumber* se codificará en *PrintableString*.
Subject Public Key	Algoritmo: RSA Encryption Longitud: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto	NO	
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora	NO	
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.1.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Registrador, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- Policy Identifier	1.3.6.1.4.1.17276.0.0.0.3.0.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/wp-content/normativapki/REG-PKI-DPC01v.3.0.3_Declaracion_de_Practicas_de_Certificacion.pdf		
-- Policy Qualifier Id (User Notice)	Declaración de Prácticas de Certificación del CORPME		
- Policy Identifier	1.3.6.1.4.1.17276.0.1.0.3.0.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/wp-content/normativapki/REG-PKI-DPC02v.3.0.3_Politicas_de_Certificacion_de_Certificados_Internos_del_CORPME.pdf		
-- Policy Qualifier Id (User Notice)	Políticas de Certificación de Certificados Internos del CORPME		
- Policy Identifier (EU Qualified Certificate)	QCP-natural-qscd (**0.4.0.194112.1.2**)		En cumplimiento de la normativa Europea 910/2014 y siguiendo las recomendaciones establecidas por la norma ETSI.

Subject Alternative Name	**Rfc822Name** = 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 **directoryName =** ➢ **1.3.6.1.4.1.17276.1.0.0.1**:*DIRECCIÓN POSTAL* ➢ **1.3.6.1.4.1.17276.1.0.0.2**: *NOMBRE* ➢ **1.3.6.1.4.1.17276.1.0.0.3**: *APELLIDO1* ➢ **1.3.6.1.4.1.17276.1.0.0.4**: *APELLIDO2* ➢ **1.3.6.1.4.1.17276.1.0.0.5**: *NIF* ➢ **1.3.6.1.4.1.17276.1.1.1.1**:*Situación del Registrador* ➢ Todos los valores se deben codificar en UTF8 ➢ Los valores especificados en MAYÚSCULAS deben ir en MAYÚSCULAS	NO	El campo 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) es opcional. [RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name 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.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registradores%20–%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Key Usage	Digital Signature Non-Repudiation Key Agreement	SI	
Extended Key Usage	Client Authentication Secure Mail Smart Card Logon	NO	
Qualified Certificate Statements	QCCompliance (**0.4.0.1862.1.1**) QcEuRetentionPeriod (**0.4.0.1862.1.3**) = 15 años QCSSCD (**0.4.0.1862.1.4**) QcPDS (**0.4.0.1862.1.5**) = http://pki.registradores.org/normativa/wp-content/normativapki/CORPME-Use_License_Registrar_210630.pdf http://pki.registradores.org/normativa/wp-content/normativapki/CORPME-Licencia_de_uso_Registrador_210630.pdf QcType-esign (**0.4.0.1862.1.6.1**)	NO	En cumplimiento de la normativa Europea 910/2014 y siguiendo las recomendaciones establecidas por la norma ETSI
QCSyntax-v2	id-etsi-qcs-SemanticsId-Natural (**0.4.0.194121.1.1**)	NO	QcSemantics para persona física.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	SI	

7.1.2.2 Certificado Cualificado de Personal Interno

A continuación, se presentan los campos y extensiones del certificado X.509 v3:

Campo / Extensión	Contenido	Crítica	Observaciones
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Validity	2 años		
Subject	Como está definido en el apartado 3.1.1.2		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. El atributo *SerialNumber* se codificará en *PrintableString*.
Subject Public Key	Algoritmo: RSA Encryption Longitud: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto	NO	
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora	NO	
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.2.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Personal Interno de los Registros, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- Policy Identifier	1.3.6.1.4.1.17276.0.0.0.3.0.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/wp-content/normativapki/REG-PKI-DPC01v.3.0.3_Declaracion_de_Practicas_de_Certificacion.pdf		

-- Policy Qualifier Id (User Notice)	Declaración de Prácticas de Certificación del CORPME		
- Policy Identifier	1.3.6.1.4.1.17276.0.1.0.3.0.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/wp-content/normativapki/REG-PKI-DPC02v.3.0.3_Politicas_de_Certificacion_de_Certificados_Internos_del_CORPME.pdf		
-- Policy Qualifier Id (User Notice)	Políticas de Certificación de Certificados Internos del CORPME		
- Policy Identifier (EU Qualified Certificate)	QCP-natural-qscd (**0.4.0.194112.1.2**)		En cumplimiento de la normativa Europea 910/2014 y siguiendo las recomendaciones establecidas por la norma ETSI.
Subject Alternative Name	**Rfc822Name** = *correo_corporativo@domain.com* **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 **directoryName =** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *DIRECCIÓN POSTAL* ➢ **1.3.6.1.4.1.17276.1.0.0.2**: *NOMBRE* ➢ **1.3.6.1.4.1.17276.1.0.0.3**: *APELLIDO1* ➢ **1.3.6.1.4.1.17276.1.0.0.4**: *APELLIDO2* ➢ **1.3.6.1.4.1.17276.1.0.0.5**: *NIF* ➢ **1.3.6.1.4.1.17276.1.1.2.1**: *Subtipo* ➢ **1.3.6.1.4.1.17276.1.1.2.2**: *ORGANIZACIÓN* ➢ **1.3.6.1.4.1.17276.1.1.2.3**: *CARGO* ➢ Todos los valores se deben codificar en UTF8 ➢ Los valores especificados en MAYÚSCULAS deben ir en MAYÚSCULAS	NO	El campo 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) es opcional. El campo 1.3.6.1.4.1.17276.1.1.2.2 (Organización) es condicional. [RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name 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.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20–%20Q2863012G, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Key Usage	Digital Signature Non Repudiation Key Agreement	SI	

Extended Key Usage	Client Authentication Secure Mail Smart Card Logon	NO	
Qualified Certificate Statements	QCCompliance (**0.4.0.1862.1.1**) QcEuRetentionPeriod (**0.4.0.1862.1.3**) = 15 años QCSSCD (**0.4.0.1862.1.4**) QcPDS (**0.4.0.1862.1.5**) = http://pki.registradores.org/normativa/wp-content/normativapki/CORPME-Licencia_de_uso_Personal_Interno_210630.pdf http://pki.registradores.org/normativa/wp-content/normativapki/CORPME-Use_License_Internal_Personnel_210630.pdf QcType-esign (**0.4.0.1862.1.6.1**)	NO	En cumplimiento de la normativa Europea 910/2014 y siguiendo las recomendaciones establecidas por la norma ETSI.
QCSyntax-v2	id-etsi-qcs-SemanticsId-Natural (**0.4.0.194121.1.1**)	NO	QcSemantics para persona física.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	SI	

7.1.2.3 Certificado Cualificado de Representante de Persona Jurídica para Facturación Electrónica

A continuación, se presentan los campos y extensiones del certificado X.509 v3:

Campo / Extensión	Contenido	Crítica	Observaciones
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Validity	2 años		
Subject	Como está definido en el apartado 3.1.1.3		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*. El atributo *SerialNumber* se codificará en *PrintableString*.
Subject Public Key	Algoritmo: RSA Encryption Longitud: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto	NO	

Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora	NO	
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.4.1		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Representante de Persona Jurídica para Facturación Electrónica, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- Policy Identifier	1.3.6.1.4.1.17276.0.0.0.3.0.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (**CPS**)	http://pki.registradores.org/normativa/wp-content/normativapki/REG-PKI-DPC01v.3.0.3_Declaracion_de_Practicas_de_Certificacion.pdf		
-- Policy Qualifier Id (User Notice)	Declaración de Prácticas de Certificación del CORPME		
- Policy Identifier	1.3.6.1.4.1.17276.0.1.0.3.0.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (**CPS**)	http://pki.registradores.org/normativa/wp-content/normativapki/REG-PKI-DPC02v.3.0.3_Politicas_de_Certificacion_de_Certificados_Internos_del_CORPME.pdf		
-- Policy Qualifier Id (User Notice)	Políticas de Certificación de Certificados Internos del CORPME		
- Policy Identifier (EU Qualified Certificate)	QCP-natural-qscd (**0.4.0.194112.1.2**)		En cumplimiento de la normativa Europea 910/2014 y siguiendo las recomendaciones establecidas por la norma ETSI.
Subject Alternative Name	**Rfc822Name** = correo_representante@domain.com **directoryName =** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *DIRECCIÓN POSTAL* ➢ **1.3.6.1.4.1.17276.1.0.0.2**: *NOMBRE* ➢ **1.3.6.1.4.1.17276.1.0.0.3**: *APELLIDO1* ➢ **1.3.6.1.4.1.17276.1.0.0.4**: *APELLIDO2* ➢ **1.3.6.1.4.1.17276.1.0.0.5**: *NIF* ➢ **1.3.6.1.4.1.17276.1.2.2.3**: *CARGO* ➢ Todos los valores se deben codificar en UTF8 ➢ Los valores especificados en MAYÚSCULAS deben ir en MAYÚSCULAS	NO	El campo 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) es opcional. [RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name 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.

CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20–%20Q2863012G, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Alternative Name (Access Location):** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Alternative Name (Access Location)** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Key Usage	Digital Signature Non Repudiation Key Agreement	SI	
Extended Key Usage	Client Authentication Secure Mail	NO	
Qualified Certificate Statements	QCCompliance (**0.4.0.1862.1.1**) QcEuRetentionPeriod (**0.4.0.1862.1.3**) = 15 años QCSSCD (**0.4.0.1862.1.4**) QcPDS (**0.4.0.1862.1.5**) = http://pki.registradores.org/normativa/wp-content/normativapki/CORPME-Licencia_de_uso_Representante_de_Persona_Juridica_para_Facturacion_Electronica_210630.pdf http://pki.registradores.org/normativa/wp-content/normativapki/CORPME-Use_License_Legal_Person_Representative_for_Electronic_Invoicing_210630.pdf QcType-esign (**0.4.0.1862.1.6.1**)	NO	En cumplimiento de la normativa Europea 910/2014 y siguiendo las recomendaciones establecidas por la norma ETSI.
QCSyntax-v2	id-etsi-qcs-SemanticsId-Natural (**0.4.0.194121.1.1**)	NO	QcSemantics para persona física.
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	SI	

7.1.2.4 Certificado No Cualificado para Procedimientos Registrales

A continuación, se presentan los campos y extensiones del certificado X.509 v3:

Campo / Extensión	Contenido	Crítica	Observaciones
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G,		Coincide con el campo asunto del certificado de la AC Subordinada Interna.

	O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Validity	3 años		
Subject	Como está definido en el apartado 3.1.1.4		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString.*
Subject Public Key	Algoritmo: RSA Encryption Longitud: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto	NO	
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora	NO	
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.3.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado No Cualificado para Procedimientos Registrales, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
Subject Alternative Name	**Rfc822Name** = *correo_responsable@domain.com* **directoryName =** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *DIRECCIÓN POSTAL* ➢ **1.3.6.1.4.1.17276.1.1.6.1:** operador ➢ Todos los valores se deben codificar en UTF8 ➢ Los valores especificados en MAYÚSCULAS deben ir en MAYÚSCULAS	NO	[RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name 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.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20INTERNA, O=Colegio%20de%20Registradores%20–%20Q2863012G, C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
8. Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Access Location:** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Access Location** (AC Subordinada Interna):	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se

	http://pki.registradores.org/certificados/ac_int_psc_corpme.crt		utilizarán los protocolos HTTP y LDAP.
Key Usage	Digital Signature Non Repudiation Key Agreement	SI	
Extended Key Usage	clientAuth serverAuth	NO	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	SI	

7.1.2.5 Certificado No Cualificado de SSL Genérico

A continuación, se presentan los campos y extensiones del certificado X.509 v3:

Campo / Extensión	Contenido	Crítica	Observaciones
Version	v3		
Serial Number			
Signature Algorithm	sha256WithRSAEncryption		OID: **1.2.840.113549.1.1.11** Norma PKCS#1 v2.1 y RFC 3447.
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Interna		Coincide con el campo asunto del certificado de la AC Subordinada Interna. Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Validity	5 años		
Subject	Como está definido en el apartado 3.1.1.5		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString.*
Subject Public Key	Algoritmo: RSA Encryption Longitud: 2048 bits		Subject Public Key Info.
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto	NO	
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora	NO	
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.1.6.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/ normativa/index.htm		

-- Policy Qualifier Id (User Notice)	Certificado No Cualificado de SSL Genérico, sujeto a la DPC del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
Subject Alternative Name	**Rfc822Name** = *correo_responsable@domain.com* **DNSName =** *al menos el nombre DNS del CN así como otros nombres DNS*	NO	[RFC5280]: Conforming implementations generating new certificates with electronic mail addresses MUST use the rfc822Name 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.
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_int_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20INTERNA,O=Colegio%20de%20Registradores%20–%20Q2863012G,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
Authority Information Access (AIA)	**Access Method:** id-ad-ocsp **Access Location:** http://ocsp.registradores.org/ **Access Method:** id-ad-calssuers **Access Location** (AC Subordinada Interna): http://pki.registradores.org/certificados/ac_int_psc_corpme.crt	NO	Las últimas versiones de Microsoft CryptoAPI no aceptan ni HTTPS ni LDAPS. Por tanto, se utilizarán los protocolos HTTP y LDAP.
KeyUsage	Digital Signature Key Encipherment Key Agreement	SI	
Extended Key Usage	clientAuth serverAuth	NO	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	SI	

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:

- Certificados Cualificados de Registradores: 1.3.6.1.4.1.17276.0.1.1.2

- Certificados Cualificados de Personal Interno: 1.3.6.1.4.1.17276.0.1.2.2
- Certificados Cualificados de Representante de Persona Jurídica para Facturación Electrónica: 1.3.6.1.4.1.17276.0.1.4.1
- Certificados No Cualificados para Procedimientos Registrales: 1.3.6.1.4.1.17276.0.1.3.2
- Certificados No Cualificados de SSL Genérico: 1.3.6.1.4.1.17276.0.1.6.2

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's

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

9.6.2 Obligaciones de las RA's

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.