Registradores DE ESPAÑA

POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS EXTERNOS DEL CORPME

Prestador del Servicio de Certificación del Colegio de Registradores

Servicio de Sistemas de la Información

26 de junio de 2017

COLEGIO DE REGISTRADORES DE ESPAÑA
Diego de León, 21 - 28006 Madrid
Tel.: +34 91 270 16 99 - Fax: +34 91 562 67 37

CONTROL DOCUMENTAL

DOCUMENTO / ARCHIVO	
Título: Políticas de Certificación de Certificados Externos del CORPME	Nombre Archivo/s: REG-PKI-DPC03v.1.1.0 Políticas de Certificación de Certificados Externos del CORPME.pdf
Código: REG-PKI-DPC03	Soporte lógico: MS-DOCX y PDF
Fecha: 26/06/2017	Ubicación física: http://pki.registradores.org/normativa/index.htm
Versión: 1.1.0	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
1.0.0	20/06/2016	Aprobación del documento
1.0.1	19/09/2016	Añadido "IDCES" a Representante con y sin pers. Jurídica. Modificaciones LFE/2016/0071
1.0.2	23/11/2016	Modificaciones (2) LFE/2016/0071
1.0.3	29/05/2017	Adaptación al Reglamento eIDAS
1.1.0	26/06/2017	Adaptación debido a la auditoría de acuerdo a las normas ETSI

ÍNDICE

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 el Art.19 de la Ley 59/2003, de Firma Electrónica, 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.*
- **ETSI TS 102 042**: *Policy requirements for certification authorities issuing public key certificates.*
- **ETSI TS 101 456**: *Policy requirements for certification authorities issuing qualified certificates.*
- **ETSI TS 102 023***: Policy requirements for time-stamping authorities.*
- **ETSI TS 101 862***: Qualified Certificate profile.*
- **ETSI TS 101 861***: Time stamping 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 319 412-5***: Certificate Profiles. QCStatements.*
- **ETSI EN 319 421***: Policy and security requirements for Trust Service Providers issuing Time-Stamps.*
- **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 (en adelante, DSCF).

La actividad del CORPME se desarrollará con plena sujeción a las prescripciones de la Ley 24/2001, de 27 de diciembre, la ley 59/2003 de Firma Electrónica, de 20 de diciembre, 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 de la DPC

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

Identificación del Documento:

Nombre del documento	Políticas de Certificación de Certificados Externos del CORPME
Versión del documento	1.1.0
Estado del documento	Versión
Fecha de emisión	26/06/2017
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.2.0.1.1.0
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.

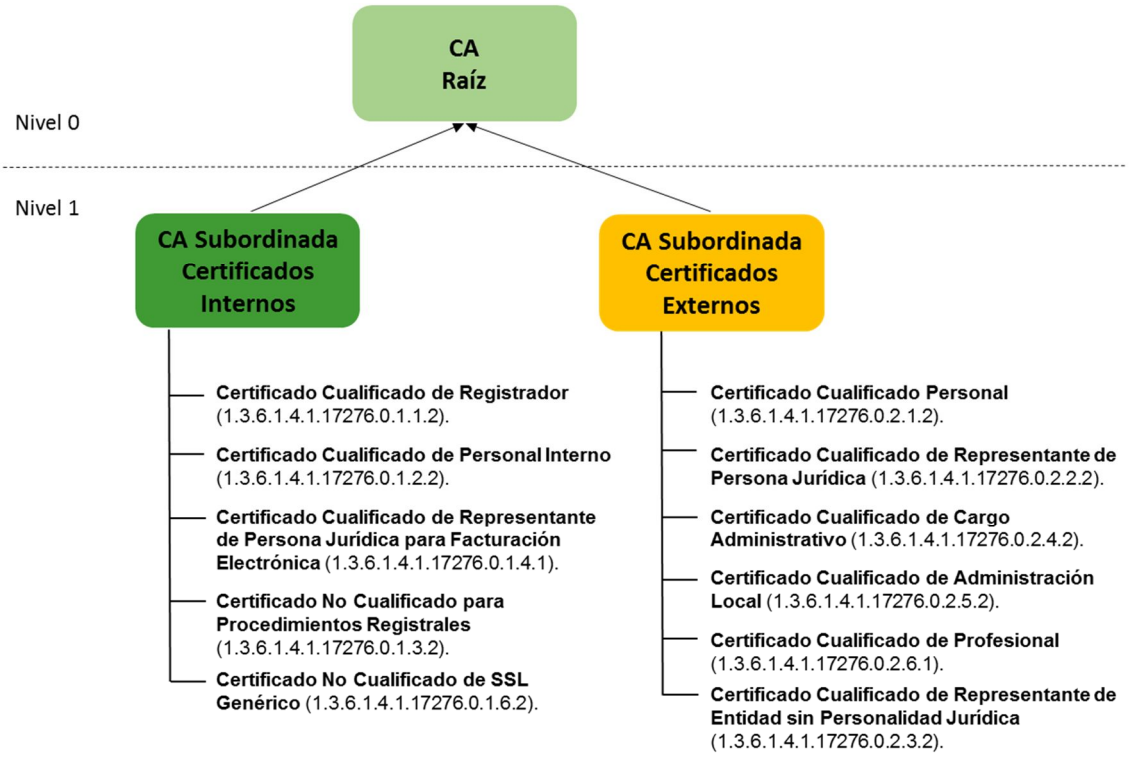
La información legal y datos identificativos del Prestador de Servicios de Certificación del CORPME estarán siempre disponibles en http://pki.registradores.org/normativa/index.htm. También podrá solicitarse una copia impresa de dicha documentación previa solicitud del interesado en la dirección siguiente:

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 59/2003, de 20 de diciembre de Firma Electrónica 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 PC afectada.

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

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

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

1.3.3 Autoridad de Certificación Raíz

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

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

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

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

Nombre distintivo	CN = 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
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
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). **TSA Certificate** (1.3.6.1.4.1.17276.0.1.10.1). **VA Certificate** (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
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://www.registradores.org/scr/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://www.registradores.org/scr/agenda**, adquiere la condición de Solicitante. La mera solicitud de un certificado no implica la concesión del mismo, la cual queda supeditada al éxito de procedimiento de Registro ante la Unidad de Tramitación correspondiente, previa verificación de la información correspondiente al certificado que el solicitante facilita.

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

1.3.8.2 Suscriptor

Se denomina suscriptor, de conformidad con lo dispuesto en el artículo 6 de la Ley 59/2003 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 figurara en el campo *Distinguished Name* del certificado digital en los campos *CN (Common Name),* SN *(Serial Number),* G *(Given Name*), S (*Surname*), , dentro de la extensión *Subject* del certificado. Los datos identificativos del Suscriptor podrán ser así mismo incluidos, dependiendo del tipo de certificado, con formato RFC6854 en una extensión de nombre alternativo *subjectAltName*, de conformidad con lo que se estipule en las políticas particulares aplicables a cada certificado.

En los casos de la representación de Personas Jurídicas o de Entidades sin Personalidad Jurídica, los datos de la representación quedarán reflejados en el apartado *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.

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
Tlf: 902181442 o 912701699

1.7 Definiciones y Acrónimos

1.7.1 Definiciones

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

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

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

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

Certificado: Documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula al Suscriptor unos Datos de verificación de Firma y confirma su identidad. En la presente 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.

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

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

Firma Electrónica 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.

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

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

Módulo Criptográfico Hardware de Seguridad (HSM): Módulo hardware utilizado para realizar funciones criptográficas y almacenar Claves en modo seguro.

Número de serie de Certificado: Valor entero y único que está asociado inequívocamente con un Certificado expedido por CORPME.

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

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

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

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

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

Prestador de Servicios de Certificación: Es aquella persona física o jurídica que, de conformidad con la legislación sobre Firma Electrónica expide certificados electrónicos, pudiendo prestar además otros servicios en relación con la Firma Electrónica. En la presente 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.

Responsable del Fichero (o del Tratamiento del Fichero): Persona que decide sobre la finalidad, contenido y uso del tratamiento de los Ficheros.

Responsable de Seguridad: Encargado de coordinar y controlar las medidas que impone el Documento de seguridad en cuanto a los Ficheros.

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

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

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

Suscriptor (o Subject): El titular o firmante del Certificado. La persona cuya identidad personal queda vinculada mediatamente a los datos firmados electrónicamente, a través de una Clave Pública certificada por el Prestador de Servicios de Certificación. El concepto de Suscriptor, será referido en los Certificados y en las aplicaciones informáticas relacionadas con su emisión como Subject, por estrictas razones de estandarización internacional.

Tarjeta criptográfica: Tarjeta utilizada por el Suscriptor para almacenar claves privadas de firma y descifrado, para generar firmas electrónicas y descifrar mensajes de datos. Tiene la consideración de 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.

PC: Política de Certificación (Certificate Policy).

PSC: Proveedor de Servicios de Certificación.

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

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

PKI: Public Key Infrastructure (Infraestructura de Clave Pública).

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

RA: Registration Authority (Autoridad de Registro).

RFC: Request For Comments. Standard desarrollado por el IETF.

ROA: Real Observatorio de la Armada Española.

SSI: Servicio de Sistemas de Información del Colegio de Registradores.

SSL: Secure Sockets Layer (Capa de Conexión Segura).

TSA: TimeStamp Authority (Autoridad de Sellado de Tiempo).

TST: TimeStamp Token (Token de Sellado de Tiempo).

TSU: TimeStamp Unit (Unidad de Sellado de Tiempo).

UTC: Universal Time Coordinated.

VA: Validation Authority (Autoridad de Validación).

2 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 Personal

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

Campo	Valor	Descripción
C	ES	País.
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 estos datos deben ir en MAYÚSCULAS.

3.1.1.2 Certificado Cualificado de Representante de Persona Jurídica

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

Campo	Valor	Descripción
C	ES	País.
description	Reg: *XXX* /Hoja: *XXX* /Tomo:*XXX* /Sección:*XXX* /Libro:*XXX* /Folio:*XXX* /Fecha: *DD-MM-AAAA* /Inscripción: *XXX*	Codificación del documento público que acredita las facultades del firmante o los datos registrales.
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).
1.3.6.1.4.1.18838.1.1	*DNI / NIE / PASAPORTE DEL REPRESENTANTE*	OID AEAT.
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 estos datos deben ir en MAYÚSCULAS. El campo tiene un tamaño máximo de 64 caracteres según la RFC 5280.

3.1.1.3 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica

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

Campo	Valor	Descripción
C	ES	País.
description	*CVE*	Codificación del documento público que acredita las facultades del firmante o los datos registrales (CVE-BOE).
organizationIdentifier	NTRES-*CÓDIGO DE LA ENTIDAD REPRESENTADA*	Código de la Entidad Representada (Requerido por @firma y ETSI 319 412-2).
O	*Denominación de la Entidad Representada*	Organización para @firma (Requerido por ETSI 319 412-2).
1.3.6.1.4.1.18838.1.1	*DNI / NIE / PASAPORTE DEL REPRESENTANTE*	OID AEAT.
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*	Todos estos datos deben ir en MAYÚSCULAS. El campo tiene un tamaño máximo de 64 caracteres según la RFC 5280.

3.1.1.4 Certificado Cualificado de Cargo Administrativo

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

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-*NIF*	NIF de la Administración.
O	*Administración Representada*	Organización.
OU	*ÓRGANO ADMINISTRATIVO*	Todos los datos deben ir en MAYÚSCULAS.
OU	*UNIDAD LOCAL*	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 APELLIDOS* – DNI *NIF*	Todos estos datos deben ir en MAYÚSCULAS. Nif del suscriptor.

3.1.1.5 Certificado Cualificado de Administración Local

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

Campo	Valor	Descripción
C	ES	País.
organizationIdentifier	VATES-*NIF*	NIF de la Administración (LAESCP).
O	*Administración Representada (Unidad Local)*	Organización.
OU	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO	Requerido por RD 668/2015. 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 APELLIDOS* – DNI *NIF*	Todos estos datos deben ir en MAYÚSCULAS.

3.1.1.6 Certificado Cualificado de Profesional

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

Campo	Valor	Descripción
C	ES	País.
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 estos datos deben ir en MAYÚSCULAS.

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 Personales, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF (compuesto por el NIF, NIE, pasaporte u otro) en el CN garantiza la unicidad del mismo.
- Para Certificados Cualificados de Representante de Persona Jurídica, el uso de la entidad (compuesto de la razón social), del NIF, del nombre (compuesto por los apellidos y el nombre), y del NIF (compuesto por el NIF, NIE, pasaporte u otro) en el CN garantiza la unicidad del mismo.
- Para Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica, el uso de la entidad (compuesto de la denominación de la entidad representada), del Identificador univoco oficial, del nombre (compuesto por los apellidos y el nombre), y del NIF (compuesto por el NIF, NIE, pasaporte u otro) en el CN garantiza la unicidad del mismo.
- Para Certificados Cualificados de Cargo Administrativo, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF (compuesto por el NIF, NIE, pasaporte u otro) en el CN garantiza la unicidad del mismo.
- Para Certificados Cualificados de Administración Local, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF (compuesto por el NIF, NIE, pasaporte u otro) en el CN garantiza la unicidad del mismo.
- Para Certificados Cualificados de Profesional, el uso del nombre (compuesto por los apellidos y el nombre), y del NIF (compuesto por el NIF, NIE, pasaporte u otro) 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 externos:

- Certificado Cualificado Personal.
- Certificado Cualificado de Representante de Persona Jurídica.
- Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica.
- Certificado Cualificado de Cargo Administrativo.
- Certificado Cualificado de Administración Local.
- Certificado Cualificado de Profesional.

Serán generadas por el dispositivo criptográfico seguro del solicitante estando bajo la custodia de éste. Dentro de estos dispositivos, 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.

3.2.2 Autenticación de la identidad de una persona jurídica o entidad sin personalidad jurídica

Los solicitantes nacionales de Certificados del CORPME, deberán comparecer ante la Unidad de Tramitación de su elección, provistos de su NIF, NIE, pasaporte u otro documento identificativo.

Los solicitantes extranjeros de Certificados del CORPME, deberán comparecer, provistos de su número de identificación de extranjeros (NIE), de su pasaporte, de su tarjeta de residencia o cualquier otro documento legal de identificación.

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, salvo para los Certificados Cualificados de Representante de Persona Jurídica, donde el Responsable de la Unidad de Tramitación podrá obtener por sus propios medios una nota acreditativa de la vigencia y datos de inscripción del cargo en el Registro Mercantil correspondiente, bien a través del servicio FLEI o a través de nota expedida por el sistema de gestión registral mercantil (si se trata de una Unidad de Tramitación sita un Registro Mercantil).

En relación con los Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica, el Responsable de la Unidad de Tramitación debe comprobar que el CVE del Boletín Oficial del Estado (BOE) es accesible y refleja el nombramiento del solicitante.

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 Personal

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF/Pasaporte/NIE) del suscriptor.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).

3.2.3.2 Certificado Cualificado de Representante de Persona Jurídica

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF/Pasaporte/NIE) del suscriptor.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Razón Social.
- NIF de la Entidad Representada.
- Cargo o apoderamiento.
    - Nota acreditativa que confirma la vigencia del cargo o apoderamiento correspondiente (este documento también se utiliza para proporcionar la información relativa a datos de inscripción). En caso de no ser aportada, el personal de la Unidad de Tramitación la obtendrá por sus propios medios, bien a través del servicio FLEI (Fichero Localizador de Empresas Inscritas) o a través de nota expedida por el sistema de gestión registral mercantil (si se trata de una Unidad de Tramitación sita un Registro Mercantil).
- Datos de inscripción.
    - Nota acreditativa que refleja la inscripción en el Registro Mercantil: Código LEI (opcional), Registro, Hoja, Tomo, Sección, Libro, Folio, Inscripción y fecha de inscripción (este documento también se utiliza para proporcionar la información relativa a cargo o apoderamiento). En caso de no ser aportada, el personal de la Unidad de Tramitación la obtendrá por sus propios medios, bien a través del servicio FLEI o a través de nota expedida por el sistema de gestión registral mercantil (si se trata de una Unidad de Tramitación sita un Registro Mercantil).

3.2.3.3 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF/Pasaporte nacional) del suscriptor.
- CVE del documento del BOE en el que se publica el otorgamiento de la representación o titularidad sobre la entidad.
- Correo electrónico.
- Número de teléfono.

- Dirección postal (opcional).
- Denominación de la Entidad Representada.
- Código de la Entidad Representada.

3.2.3.4 Certificado Cualificado de Cargo Administrativo

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF/Pasaporte nacional) del suscriptor.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Cargo administrativo que ostenta, correspondiente con su categoría.
    - Certificado que confirma la vigencia del cargo que ostenta.
- Denominación de la Administración Representada.
- NIF de la Administración Representada.
- Órgano administrativo representado.
- Denominación de la Unidad local.

3.2.3.5 Certificado Cualificado de Administración Local

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF/Pasaporte/NIE) del suscriptor.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Cargo administrativo que ostenta, correspondiente con su categoría.
    - Certificado que confirma la vigencia del cargo que ostenta.
- NIF de la Administración Local.
- Provincia de la Administración Local.
- Denominación de la Unidad local.

3.2.3.6 Certificado Cualificado de Profesional

- Nombre y apellidos del suscriptor.
- Documento identificativo (DNI/NIF/Pasaporte nacional) del suscriptor.
- Correo electrónico.
- Número de teléfono.
- Dirección postal (opcional).
- Profesión, entendida como el Colectivo Profesional al que está adscrito el solicitante del certificado.
    - Certificado que confirma la profesión correspondiente, emitido por un Colegio o Asociación Profesional.

3.2.3.7 Autenticación de la identidad de un dispositivo

No estipulado.

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, salvo para los Certificados Cualificados de Representante de Persona Jurídica, donde el Responsable de la Unidad de Tramitación podrá obtener por sus propios medios una nota acreditativa de la vigencia y datos de inscripción del cargo en el Registro Mercantil correspondiente, bien a través del servicio FLEI o a través de nota expedida por el sistema de gestión registral mercantil (si se trata de una Unidad de Tramitación sita un Registro Mercantil).

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.

Adicionalmente a lo indicado en los siguientes apartados, se podrá efectuar una solicitud de certificado por parte del representante legal del suscriptor, debidamente autorizado.

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 Personal

La solicitud de este tipo de certificados se podrá efectuar por cualquier persona mayor de edad.

El proceso de solicitud requiere de cita previa. En estos casos, como paso previo a la obtención del certificado, el solicitante se conecta a la página web https://www.registradores.org/scr/agenda. En caso de no estar dado de alta en el sistema, se debe de registrar como usuario del mismo. Una vez registrado debe cumplimentar un formulario en línea, con la información necesaria (día y hora en la Unidad de Tramitación elegida) para la expedición del certificado, a partir de la cual se rellenarán los campos del mismo y se generará la licencia de uso del certificado.

Dado que la licencia de uso del certificado deberá ser firmada por el Responsable de la Unidad de Tramitación, es imperativo que la comparecencia personal del solicitante coincida con la presencia del mismo, por ello el solicitante deberá seleccionar día y hora, de entre los disponibles y previamente habilitados como hábiles para la expedición de certificados digitales. Una vez fijada fecha y hora para la comparecencia, el solicitante recibirá por correo electrónico un justificante de la cita concertada.

4.1.1.2 Certificado Cualificado de Representante de Persona Jurídica

La solicitud de este tipo de certificados se podrá efectuar por parte de los cargos de entidades inscritas en los Registros Mercantiles.

El proceso de solicitud requiere de cita previa. En estos casos, como paso previo a la obtención del certificado, el solicitante se conecta a la página web https://www.registradores.org/scr/agenda. En caso de no estar dado de alta en el sistema, se debe de registrar como usuario del mismo. Una vez registrado debe cumplimentar un formulario en línea, con la información necesaria (día y hora en la Unidad de Tramitación elegida) para la expedición del certificado, a partir de la cual se rellenarán los campos del mismo y se generará la licencia de uso del certificado.

Dado que la licencia de uso del certificado deberá ser firmada por el Responsable de la Unidad de Tramitación, es imperativo que la comparecencia personal del solicitante coincida con la presencia del mismo, por ello el solicitante deberá seleccionar día y hora, de entre los disponibles y previamente habilitados como hábiles para la expedición de certificados digitales. Una vez fijada fecha y hora para la comparecencia, el solicitante recibirá por correo electrónico un justificante de la cita concertada.

4.1.1.3 Certificado Cualificado de Representante de Persona sin Entidad Jurídica

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

El proceso de solicitud requiere de cita previa. En estos casos, como paso previo a la obtención del certificado, el solicitante se conecta a la página web https://www.registradores.org/scr/agenda. En caso de no estar dado de alta en el sistema, se debe de registrar como usuario del mismo. Una vez registrado debe cumplimentar un formulario en línea, con la información necesaria (día y hora en la Unidad de Tramitación elegida) para la expedición del certificado, a partir de la cual se rellenarán los campos del mismo y se generará la licencia de uso del certificado.

Dado que la licencia de uso del certificado deberá ser firmada por el Responsable de la Unidad de Tramitación, es imperativo que la comparecencia personal del solicitante coincida con la presencia del mismo, por ello el solicitante deberá seleccionar día y hora, de entre los disponibles y previamente habilitados como hábiles para la expedición de certificados digitales. Una vez fijada fecha y hora para la comparecencia, el solicitante recibirá por correo electrónico un justificante de la cita concertada.

4.1.1.4 Certificado Cualificado de Cargo Administrativo

La solicitud de este tipo de certificados se podrá efectuar por parte de los cargos de la administración pública.

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.

4.1.1.5 Certificado Cualificado de Administración Local

La solicitud de este tipo de certificados se podrá efectuar por parte del personal adscrito a la administración local.

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.

4.1.1.6 Certificado Cualificado de Profesional

La solicitud de este tipo de certificados se podrá efectuar por parte del personal perteneciente a un colegio o asociación profesional con convenio con el prestador.

El proceso de solicitud requiere de cita previa. En estos casos, como paso previo a la obtención del certificado, el solicitante se conecta a la página web https://www.registradores.org/scr/agenda. En caso de no estar dado de alta en el sistema, se debe de registrar como usuario del mismo. Una vez registrado debe cumplimentar un formulario en línea, con la información necesaria (día y hora en la Unidad de Tramitación elegida) para la expedición del certificado, a partir de la cual se rellenarán los campos del mismo y se generará la licencia de uso del certificado.

Dado que la licencia de uso del certificado deberá ser firmada por el Responsable de la Unidad de Tramitación, es imperativo que la comparecencia personal del solicitante coincida con la presencia del mismo, por ello el solicitante deberá seleccionar día y hora, de entre los disponibles y previamente habilitados como hábiles para la expedición de certificados digitales. Una vez fijada fecha y hora para la comparecencia, el solicitante recibirá por correo electrónico un justificante de la cita concertada.

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 las claves cambiadas

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

4.7.6 Publicación del certificado con las nuevas claves por la CA

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

4.7.7 Notificación de la 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 Controles Físicos

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

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, son generadas siempre durante la comparecencia del solicitante en la Unidad de Tramitación y con su intervención personal en el proceso de asignación de claves. La generación se realiza en todo caso dentro de un dispositivo criptográfico con un nivel de seguridad certificado como: FIPS 140-1 nivel 2, o superior, CC EAL4+ u otro con características análogas.

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

La clave pública de los certificados de funcionario público se genera en el dispositivo criptográfico del titular en el puesto de emisión siendo la RA la responsable de entregar dicha clave pública a la CA.

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

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

6.1.5 Tamaño de las claves

El tamaño de las claves de la CA de Certificados Externos 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 externos está codificada de acuerdo con RFC6818.

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

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

6.2 Protección de la clave privada y controles de ingeniería de los módulos

6.2.1 Estándares para los módulos criptográficos

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

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

Las claves privadas de los certificados externos 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 externos 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 externos para garantizar el no repudio.

6.2.5 Archivado de la clave privada

Las claves privadas de firma de los certificados externos 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 externos 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 externos 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 externos es de dos (2) años desde el momento de emisión del mismo.

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 externos y se emiten de acuerdo con el estándar de la Unión Internacional de Telecomunicaciones, número X-509, versión 3.

7.1.2 Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- *Subject Key Identifier*
- *Certificate Policies*
- *Basic Constraints*
- *Key Usage*
- *Thumbprint algorithm*
- *Thumbprint*
- *Subject Alternative Names*
- *CRL Distribution Points*
- *Extensiones de certificado cualificado EU (EU-qualified)*
    - *Qualified Certificate Statements*
    - *QCSyntax v2*
    - *EU Qualified Certificate Policy Identifier*

7.1.2.1 Certificado Cualificado Personal

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

Campo	Contenido Propuesto	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.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles,		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.

	CN=Autoridad de Certificación de los Registradores - AC Externa		
Valid from			Fecha de inicio del periodo de validez.
Valid to			Fecha de final del periodo de validez.
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*.
Public key	Algoritmo: RSA Encryption Longitud: 2048 bits		
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto		
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora		
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1. 17276.0.2.1.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado Personal, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- 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_personal@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* ➢ Los valores se deben codificar en UTF8	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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20EXTERNA, 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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) = https://pki.registradores.org/normativa/en/tsp_information.htm 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.
Restricciones básicas	Subject Type=End Entity Path Length Constraint=None	SI	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.2 Certificado Cualificado de Representante de Persona Jurídica

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

Campo	Contenido Propuesto	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.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles,		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.

	CN=Autoridad de Certificación de los Registradores - AC Externa		
Valid from			Fecha de inicio del periodo de validez.
Valid to			Fecha de final del periodo de validez.
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*.
Public key	Algoritmo: RSA Encryption Longitud: 2048 bits		
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto		
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora		
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.2.2.2		
- 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, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- 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.
- Policy Identifier	2.16.724.1.3.5.8		Certificado de representante de persona jurídica cualificado por el Ministerio de Hacienda.
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* ➢ **1.3.6.1.4.1.17276.1.2.2.4**: *Datos de Inscripción: Código LEI* ➢ **1.3.6.1.4.1.17276.1.2.2.5**: *Código Registro* ➢ **1.3.6.1.4.1.17276.1.2.2.6**: *Hoja* ➢ **1.3.6.1.4.1.17276.1.2.2.7**: *Tomo*	NO	Los campos 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) y 1.3.6.1.4.1.17276.1.2.2.4 (Datos de Inscripción: Código LEI) son opcionales. [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.

	➢ **1.3.6.1.4.1.17276.1.2.2.8**: *Sección* ➢ **1.3.6.1.4.1.17276.1.2.2.9**: *Libro* ➢ **1.3.6.1.4.1.17276.1.2.2.10**: *Folio* ➢ **1.3.6.1.4.1.**17276.**1.2.2.11**: *Inscripción* ➢ Los valores se deben codificar en UTF8		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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20EXTERNA, 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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) = https://pki.registradores.org/normativa/en/tsp_information.htm 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.
Restricciones básicas	Subject Type=End Entity Path Length Constraint=None	SI	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.3 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica

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

Campo	Contenido Propuesto	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.

Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Valid from			Fecha de inicio del periodo de validez.
Valid to			Fecha de final del periodo de validez.
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*.
Public key	Algoritmo: RSA Encryption Longitud: 2048 bits		
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto		
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora		
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.2.6.1		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- 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.
- Policy Identifier	2.16.724.1.3.5.9		Certificado de representante de entidad sin personalidad jurídica cualificado por el Ministerio de Hacienda.
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*	NO	El campo 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) es opcional.

	➢ **1.3.6.1.4.1.17276.1.2.6.1**: *Cargo* ➢ Los valores se deben codificar en UTF8		[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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20EXTERNA, 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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) = https://pki.registradores.org/normativa/en/tsp_information.htm 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.
Restricciones básicas	Subject Type=End Entity Path Length Constraint=None	SI	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.4 Certificado Cualificado de Cargo Administrativo

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

Campo	Contenido Propuesto	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.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Valid from			Fecha de inicio del periodo de validez.
Valid to			Fecha de final del periodo de validez.
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*. El atributo *SerialNumber* se codificará en *PrintableString*.
Public key	Algoritmo: RSA Encryption Longitud: 2048 bits		
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto		
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora		
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1. 17276.0.2.3.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Cargo Administrativo, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- 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_cargo@domain.com **directoryName =** ➢ **1.3.6.1.4.1.17276.1.0.0.1**: *Dirección Postal*	NO	El campo 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) es opcional.

	➢ **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* ➢ **1.3.6.1.4.1.17276.1.2.3.1**: *Cargo Administrativo* ➢ **1.3.6.1.4.1.17276.1.2.3.2**: *Administración* ➢ **1.3.6.1.4.1.17276.1.2.3.3**: *Órgano administrativo representado* ➢ **1.3.6.1.4.1.17276.1.2.3.4**: *Unidad local* ➢ Los valores se deben codificar en UTF8		[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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/CN=AC%20EXTERNA,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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) = https://pki.registradores.org/normativa/en/tsp_information.htm 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.
Restricciones básicas	Subject Type=End Entity Path Length Constraint=None	SI	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.5 Certificado Cualificado de Administración Local

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

Campo	Contenido Propuesto	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.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Valid from			Fecha de inicio del periodo de validez.
Valid to			Fecha de final del periodo de validez.
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*. El atributo *SerialNumber* se codificará en *PrintableString*.
Public key	Algoritmo: RSA Encryption Longitud: 2048 bits		
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto		
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora		
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1. 17276.0.2.4.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Administración Local, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.
- 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_cargo@domain.com **directoryName =** ➢ **1.3.6.1.4.1.17276.1.2.4.1**: *Cargo local*	NO	El campo 1.3.6.1.4.1.17276.1.0.0.1 (Dirección Postal) es opcional.

	➢ **1.3.6.1.4.1.17276.1.2.4.2**: *Provincia de la Administración Local* ➢ **1.3.6.1.4.1.17276.1.2.4.3**: *Unidad local* ➢ **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* ➢ **2.16.724.1.3.5.7.1.1:** CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO ➢ **2.16.724.1.3.5.7.1.2:** *Entidad propietaria* ➢ **2.16.724.1.3.5.7.1.3:** *NIF Entidad Propietaria* ➢ **2.16.724.1.3.5.7.1.4:** *DNI del responsable del certificado* ➢ **2.16.724.1.3.5.7.1.6:** *Nombre* ➢ **2.16.724.1.3.5.7.1.7:** *Apellido1* ➢ **2.16.724.1.3.5.7.1.8:** *Apellido2* ➢ Los valores se deben codificar en UTF8		[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. Requerido por RD 668/2015 (LAESCP).
CRL Distribution Points	**(1) HTTP:** http://pki.registradores.org/crls/crl_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20EXTERNA, 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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) = https://pki.registradores.org/normativa/en/tsp_information.htm 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.
Restricciones básicas	Subject Type=End Entity Path Length Constraint=None	SI	
Thumbprint algorithm	sha1		
Thumbprint			

7.1.2.6 Certificado Cualificado de Profesional

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

Campo	Contenido Propuesto	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.
Signature hash algorithm	sha256		
Issuer	C=ES, organizationIdentifier=VATES-Q2863012G, O=Colegio de Registradores de la Propiedad y Mercantiles, CN=Autoridad de Certificación de los Registradores - AC Externa		Todos los *DirectoryString* codificados en UTF8. El atributo "C" (*countryName*) se codificará de acuerdo a "*ISO 3166-1-alpha-2 code elements*", en *PrintableString*.
Valid from			Fecha de inicio del periodo de validez.
Valid to			Fecha de final del periodo de validez.
Subject	Como está definido en el apartado 3.1.1.6.		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*.
Public key	Algoritmo: RSA Encryption Longitud: 2048 bits		
Subject Key Identifier	Función hash sha1 sobre la clave pública del sujeto		
Authority Key Identifier	Función hash sha1 sobre la clave pública de la CA emisora		
Certificate Policies	Se utilizará	NO	
- Policy Identifier	1.3.6.1.4.1.17276.0.2.5.2		
- Policy Qualifier Info			
-- Policy Qualifier Id (CPS)	http://pki.registradores.org/normativa/index.htm		
-- Policy Qualifier Id (User Notice)	Certificado Cualificado de Profesional, sujeto a la Declaración de Prácticas de Certificación del Colegio de Registradores de la Propiedad y Mercantiles de España (© 2016)		Campo codificado en UTF8.

- 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_profesional@domain.com **directoryName =** ➢ **1.3.6.1.4.1.17276.1.2.5.1**: *Colectivo profesional al que está adscrito el titular del certificado* ➢ **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* ➢ Los valores se deben codificar en UTF8	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_ext_psc_corpme.crl **(2) LDAP:** ldap://ldap.registradores.org/ CN=AC%20EXTERNA, 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 Externa): http://pki.registradores.org/certificados/ac_ext_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	
Enhanced 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**) = https://pki.registradores.org/normativa/en/tsp_information.htm 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.
Restricciones básicas	Subject Type=End Entity Path Length Constraint=None	SI	
Thumbprint algorithm	sha1		
Thumbprint			

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 externos 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 Personales: 1.3.6.1.4.1.17276.0.2.1.2
- Certificados Cualificados de Representante de Persona Jurídica: 1.3.6.1.4.1.17276.0.2.2.2
- Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica: 1.3.6.1.4.1.17276.0.2.6.1
- Certificados Cualificados de Cargo Administrativo: 1.3.6.1.4.1.17276.0.2.3.2
- Certificados Cualificados de Administración local: 1.3.6.1.4.1.17276.0.2.4.2
- Certificados Cualificados de Profesional: 1.3.6.1.4.1.17276.0.2.5.2

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.