Registradores DE ESPAÑA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Prestador del Servicio de Certificación del Colegio de Registradores

Servicio de Sistemas de la Información
29 de mayo de 2017

Registradores DE ESPAÑA
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: Declaración de Prácticas de Certificación	Nombre Archivo/s: REG-PKI-DPC01v.1.0.4 Declaración de Prácticas de Certificación.pdf
Código: REG-PKI-DPC01	Soporte lógico: MS-DOCX y PDF
Fecha: 29/05/2017	Ubicación física: http://pki.registradores.org/normativa/index.htm
Versión: 1.0.4	

REGISTRO DE CAMBIOS		
Versión	**Fecha**	**Motivo del cambio**
0.0.1	08/06/2016	Versión inicial debido a la renovación de la PKI.
0.0.2	20/06/2016	Revisión del documento y corrección de errores.
1.0.0	20/06/2016	Aprobación del documento
1.0.1	19/09/2016	Modificación LFE/2016/0071
1.0.2	23/11/2016	Modificación (2) LFE/2016/0071
1.0.3	23/12/2016	Modificación (3) LFE/2016/0071
1.0.4	29/05/2017	Adaptación al Reglamento eIDAS

DISTRIBUCIÓN DEL DOCUMENTO	
Nombre	**Área**
Público	Público / Internet

CONTROL DEL DOCUMENTO			
PREPARADO	**REVISADO**	**APROBADO**	**ACEPTADO**
PwC	Óscar Yagüe	Raúl Avedillo	Luis Alberto Lahoz
29/05/2017	29/05/2017	29/05/2017	29/05/2017

ÍNDICE

1 INTRODUCCIÓN

1.1 Presentación

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

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

La Declaración de Prácticas de Certificación (en adelante, DPC), emitida de conformidad con el Art.19 de la Ley 59/2003, de Firma Electrónica, 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 presente DPC. En caso de conflicto o contradicción entre lo dispuesto en la Declaración de Prácticas de Certificación y las citadas Políticas, prevalecerá lo preceptuado en estas últimas.

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

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 DPC 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 Emisión de certificados SET de pruebas

El Prestador de Servicios de Confianza de CORPME realiza la emisión de un conjunto de certificados de pruebas para que tanto el organismo regulador en procesos de inspección o registro de nuevos certificados, como los desarrolladores de aplicaciones en proceso de integración o de evaluación para su aceptación, tengan a su disposición certificados de la jerarquía real con datos ficticios.

A continuación, se proporcionan los datos residentes en dichos certificados para que terceros que confían en la Jerarquía de certificación de CORPME puedan comprobar que se trata de certificados de pruebas sin responsabilidad:

Nombre de la entidad	[PRUEBAS] ENTIDAD
NIF de la Entidad (organizationIdentifier)	B00000000
Dirección Postal	DOMICILIO, 28001
Nombre	NOMBRE
Primer Apellido	APELLIDO1
Segundo Apellido	APELLIDO2
DNI	00000000T
CVE (BOE)	000000000
Representación de Entidad con Personalidad Jurídica	B00000000
DNS	pruebas.corpme.es
Mail	pruebas@corpme.es
Sociedad Colegial	SOCIEDAD COLEGIAL
Administración Local	ADMINISTRACIÓN LOCAL
Cargo Administrativo	CARGO
Profesión	PROFESION

No todos los datos aquí mostrados se reflejan en todos los certificados emitidos bajo los perfiles que cubren tanto esta DPC como las PC's asociadas, sino que se utilizan en función de su aplicabilidad al perfil de certificación correspondiente.

En casos como los indicados, se dispone de las mismas versiones de certificados tanto en formato físico (claves generadas en dispositivos criptográficos seguros) como en formato PKCS#12 (formato software de almacenamiento de claves). La prueba de posesión de la clave privada queda custodiada en ambos casos por el SSI del Prestador de Servicios de Confianza de CORPME.

Es importante reseñar que las pruebas para desarrolladores se realizarán preferentemente con la jerarquía de pruebas del PSC del CORPME y sólo se suministrarán en caso de justificada necesidad para evitar la propagación de este set de pruebas. Asimismo se revocarán tan pronto determine el propio PSC del CORPME.

1.3 Generalidades de la DPC

La presente DPC se emite teniendo en cuenta las recomendaciones de la (Request for comments) RFC3647: Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, de IETF.

El CORPME no emitirá certificados de Persona Jurídica en tanto por mandato legal no se establezca la obligatoriedad, a cargo de los Prestadores de Servicios de Certificación que emitan certificados cualificados, de expedir tal tipo de certificados, salvo en aquellos perfiles donde explícitamente se determinen en el presente documento y en las propias PC's.

La expedición de certificados digitales a otras entidades o corporaciones que deseen actuar como Autoridades de Certificación subordinadas o secundarias, emitiendo certificados digitales bajo la jerarquía del Certificado Raíz del CORPME, requerirá el acuerdo expreso de la Comisión Directora, órgano máximo directivo del CORPME.

Cuando no se haya previsto nada en alguna sección aparecerá la frase "No estipulado".

1.4 Nombre del documento e Identificación de la DPC

El presente documento se denomina *DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL CORPME.*

Identificación del Documento:

Nombre del documento	Declaración de Prácticas de Certificación del CORPME
Versión del documento	1.0.4
Estado del documento	Versión
Fecha de emisión	29/05/2017
Fecha de expiración	No aplicable
OID (Object Identifier)	1.3.6.1.4.1.17276.0.0.0.1.0.4
Ubicación de la DPC	http://pki.registradores.org/normativa/index.htm

1.5 Participantes en la Infraestructura de Clave Pública (PKI) del Prestador del Servicio de Certificación del Colegio de Registradores

1.5.1 Prestador de Servicios de Certificación (PSC)

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

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

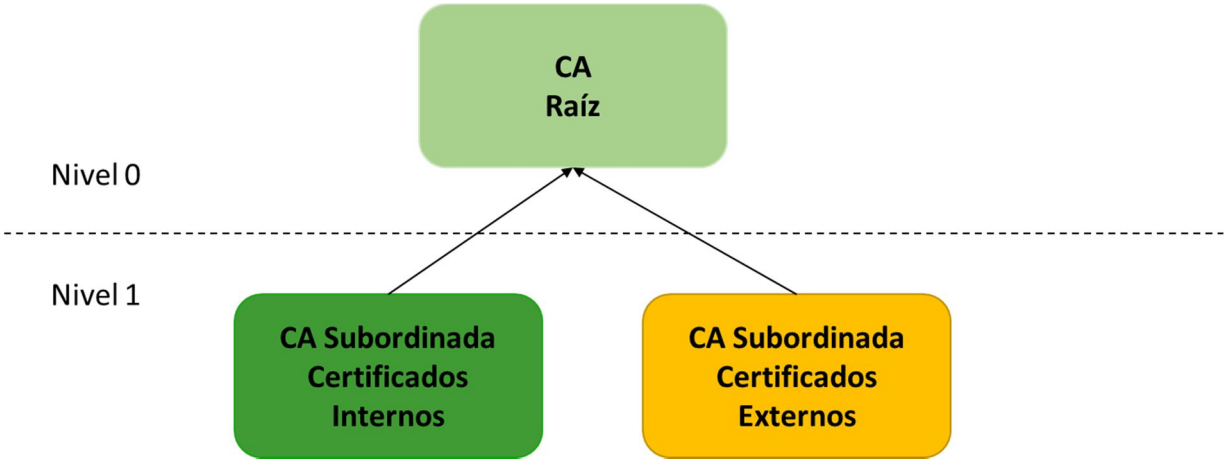
Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España
Prestador del Servicio de Certificación del Colegio de Registradores
C/ DIEGO DE LEON, 21.
28006-MADRID

En el CORPME concurre, además de la condición de PSC, la de CA (Certification Authority), desarrollando su actividad de conformidad con la legislación vigente en la materia, concretamente, la ley 59/2003, de 20 de diciembre de Firma Electrónica y el reglamento EU 910/2014 sobre identificación electrónica y servicios de confianza.

El PSC posee un Sistema de Gestión Integrado de Calidad y de Seguridad de la Información para todos los servicios de certificación del CORPME.

Un parte importante de dicho Sistema de Gestión Integrado es el análisis y tratamiento de riesgos. El PSC cuenta con una Metodología de Análisis y Gestión de Riesgos, mediante la cual se realiza el análisis de los riesgos para todos los activos de información relativos a la prestación de servicios de certificación, se evalúan los requisitos de negocio y se determinan los requisitos de seguridad. Los riesgos se revisan periódicamente y se procede a mitigarlos mediante un Plan de Tratamiento.

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



1.5.2 Autoridad de Aprobación de Políticas

La Autoridad de Aprobación de Políticas (en adelante, AAP) es la organización responsable de la aprobación de la presente 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.

1.5.3 Autoridad de Certificación Raíz

El CORPME emite todos los certificados objeto de la presente 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

1.5.4 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 Certificado Cualificado para Personal Interno Certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica Certificado No Cualificado para Procedimientos Registrales Certificado No Cualificado de SSL Genérico

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 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

1.5.5 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.

1.5.6 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).

1.5.7 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.

1.5.8 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.

1.5.8.1 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.

1.5.8.2 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.

1.5.8.3 Tercero que confía en los Certificados de CORPME

A los efectos de esta DPC, 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.

1.6 Clases de Certificados Digitales y límites para su uso

Los certificados digitales emitidos por CORPME son de varios tipos:

- **Certificados propios de la PKI**
  - Certificado CA Raíz
  - Certificado CA Subordinada Externa
  - Certificado CA Subordinada Interna
  - Certificado VA
  - Certificado TSA
  - Certificados de Operadores de Registro
- **Certificados Personales:**
  - Certificados internos:
    - Certificado Cualificado de Registrador
    - Certificado Cualificado para Personal Interno
    - Certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica
  - 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
- **Certificados de Dispositivos**

- Certificado No Cualificado para Procedimientos Registrales

- **Certificados de Componente**
  - Certificado No Cualificado de SSL Genérico

1.6.1 Certificados Propios de la PKI

Son los certificados que respaldan las claves privadas utilizadas por el Servicio para la firma de certificados y son los siguientes: el certificado raíz y los de jerarquía. El Certificado de la clave principal o raíz es el certificado *auto-firmado* en el que se inicia la cadena de confianza. Directamente subordinados, se encuentran los certificados de jerarquía, que serán uno para los certificados internos y otro para los externos.

Estos certificados tendrán una longitud de clave igual o mayor de 2048 bits (siendo igual a 4096 bits para el caso de los certificados de las Autoridades de Certificación Raíz y Subordinadas) y una vigencia de doce (12) años, salvo para la CA Raíz, que será de veinticuatro (24) años. El titular de las claves del servicio es el propio CORPME y se emiten y revocan por la Unidad de Tramitación Central, a solicitud de la Comisión Directora.

1.6.1.1 Certificado VA

Aquel certificado utilizado por la Autoridad de Validación para firmar las respuestas relativas a la comprobación del estado de los certificados emitidos por el PSC del CORPME.

1.6.1.2 Certificado TSA

Aquel certificado utilizado por la TSA para firmar el sello de tiempo.

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.

1.6.2 Certificados de Operador de Registro

Los Certificados de Operador de Registro son certificados de uso personal utilizados por los operadores adscritos a las Unidades de Tramitación para su utilización en el ejercicio de la actividad certificadora. Todos estos certificados estarán emitidos dentro los perfiles de certificación de Certificado Cualificado para Personal Interno y/o Certificado Cualificado de Registrador. Todas y cada una de las acciones realizadas sobre los certificados se autorizan mediante una orden que debe estar firmada con una clave respaldada por un certificado de operador.

Se distinguen en esta clase dos categorías de certificados:

- Operador de la Unidad de Tramitación Central
- Operador de los Registros

Los Certificados de Operador de los Registros contienen el nombre y dirección de correo electrónico del titular, el nombre de la Unidad de destino y su dirección postal. La longitud de las

claves certificadas será como mínimo de 2048 bits y la vigencia de los certificados de dos (2) años. Su titular es el operador y se emiten y revocan por la Unidad de Tramitación Central, a petición de la Comisión Directora en el caso de los operadores de esta misma Unidad y a petición de los Registradores, en el caso de los operadores de las Unidades de Tramitación de los Registros.

1.6.3 Certificados para las comunicaciones del Servicio

Son aquellos destinados a su uso por los procesos automatizados que se utilizan en las comunicaciones del Servicio con las Unidades de Tramitación o con los usuarios. La longitud de las claves certificadas será de 2048 bits y la vigencia de los certificados de dos (2) años. El titular es el propio PSC del CORPME y se emiten y revocan por la Unidad de Tramitación Central, a petición de la Comisión Directora.

1.6.4 Certificados Personales

1.6.4.1 Certificados Internos

Los certificados internos tienen carácter profesional y se ponen a disposición de su titular únicamente para su uso en actividades relacionadas con su función dentro de la organización registral.

1.6.4.1.1 Certificado Cualificado de Registrador

Los Certificados Cualificados de Registradores son certificados para uso personal que acreditan la identidad de su titular, así como su condición de Registrador y en su caso, liquidador de impuestos en ejercicio y el Registro, punto de registro, o en su caso, la Oficina Liquidadora donde desarrolla su actividad. También incluirá indicación del destino administrativo especial en que se encuentre el Registrador. Los Certificados Cualificados de Registradores se emiten para el exclusivo uso en el ámbito de dichas funciones.

Las firmas respaldadas por estos certificados acreditan la intervención personal del Registrador en todos los actos que le son propios de su función, incluyendo toda relación con terceros y estén previstos en las leyes, así como en la elaboración de todo tipo de documento o certificaciones en formato electrónico. Se emiten para el exclusivo uso en el ámbito de dichas funciones y relaciones con las Administraciones Públicas.

Los Certificados Cualificados de Registradores se utilizan en las comunicaciones internas de los Registros, así como para autorizar las solicitudes que el Registrador deba enviar a la Unidad de Tramitación Central. También podrán ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso.

Los Certificados Cualificados de Registradores contienen el nombre del Registrador suscriptor del certificado y su número de identificación fiscal, así como la dirección de correo electrónico del suscriptor, el nombre del Registro de destino y su dirección postal.

1.6.4.1.2 Certificado Cualificado para Personal Interno

Los Certificados Cualificados para Personal Interno son certificados para uso personal que acreditan la identidad de su titular, así como su condición de empleado del Registro, Colegio, Decanato, Sociedad del Colegio o empleados en situaciones especiales. Se trata de certificados para uso interno y para relaciones con las Administraciones Públicas.

Los Certificados Cualificados para Personal Interno contienen el nombre del empleado suscriptor del certificado y su dirección de correo electrónico, así como el nombre del Registro o Unidad de destino y su dirección postal.

1.6.4.1.3 Certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica

El certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica acredita la identidad de su titular, que será siempre una persona física, y su condición de representante de una persona jurídica que será siempre, el Colegio de Registradores, y su condición de miembro de la Junta de Gobierno. Únicamente podrán ser utilizados para firmar los documentos relativos a la facturación electrónica y su uso está limitado a la firma de facturas.

Además de la identificación del Suscriptor y del Colegio de Registradores como entidad jurídica, contendrá información sobre la relación del Suscriptor con la Sociedad reflejando su cargo dentro de la Junta de Gobierno.

La Unidad de Tramitación Central del CORPME emitirá estos certificados bajo solicitud aprobada según el procedimiento de gestión de solicitudes y validada esta solicitud por el Director Técnico del SSI del CORPME

1.6.4.2 Certificados Externos

Salvo que en las PC's particulares se establezca lo contrario, los certificados emitidos bajo la clave secundaria para certificados externos podrán utilizarse únicamente en los actos inscribibles y en las comunicaciones que se efectúen entre su titular y los Registros, Administraciones Públicas y otro tipo de Organismos y Entidades, de conformidad con lo dispuesto en su respectiva PC.

El suscriptor habrá de abstenerse de emplearlos para otro fin distinto al autorizado y, de no cumplirse esta obligación, en ningún caso las firmas respaldadas por estos certificados tendrán efectos frente a terceros. Esta circunstancia se hará constar expresamente en el propio contenido de los certificados.

Los certificados externos serán autorizados y revocados por las Unidades de Tramitación, de acuerdo con el procedimiento establecido para cada una de sus clases.

1.6.4.2.1 Certificado Cualificado Personal

Los Certificados Cualificados Personales acreditan la identidad de su titular, que será siempre una persona física. Únicamente podrán ser utilizados para firmar los documentos que se presenten ante los Registros, Administraciones Públicas y otros tipos de Organismos y Entidades, así como en las comunicaciones que se realicen con los mismos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. También pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y la firma de correos electrónicos.

Los Certificados Cualificados Personales tienen como finalidad principal la firma de documentos, garantizando la autenticidad del emisor de la comunicación, el no repudio de origen y la integridad del contenido. Los Certificados Personales también pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso.

Los Certificados Cualificados Personales identificarán a su titular en los diferentes campos del atributo campo DN (*Distinguished name=nombre distintivo*) que contiene: el nombre, apellidos y número de identificación fiscal (NIF, NIE, pasaporte u otro), sin que se admita el uso de seudónimos.

En defecto de NIF, podrá incluirse el número del documento nacional de identidad o, tratándose de extranjeros, el número de identificación de extranjeros, el de su pasaporte, el de su tarjeta de residencia o el de cualquier otro documento legal de identificación.

También podrán constar en el certificado la dirección, los números de teléfono y fax, y la dirección de correo electrónico del suscriptor, según se disponga en la correspondiente PC.

1.6.4.2.2 Certificado Cualificado de Representante de Persona Jurídica

Los Certificados Cualificados de Representante de Persona Jurídica acreditan la identidad de su titular, que será siempre una persona física, y su condición de representante orgánico o voluntario de una persona jurídica. Se emiten para su utilización, de manera principal y de conformidad con las políticas particulares de certificación, para la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Representante de Persona Jurídica también pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y la firma de correos electrónicos.

El Certificado Cualificado de Representante de Persona Jurídica además de la identificación del Suscriptor y de la Sociedad, contendrá información sobre la relación de representación que ostenta el suscriptor respecto de la Sociedad Representada. Estos certificados contendrán los datos de Inscripción que consten en el momento de la emisión en el Registro Mercantil.

En caso de disconformidad entre los datos de representación incorporados en el certificado y los obrantes en el Registro Mercantil, prevalecerán siempre estos últimos.

1.6.4.2.3 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica

Los Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica acreditan la identidad de su titular, que será siempre una persona física, y su condición de titular o representante orgánico o voluntario de una Entidad sin personalidad jurídica registrada. Se emiten para su utilización, de manera principal y de conformidad con las políticas particulares de certificación, para la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Representante de Entidad sin Personalidad Jurídica también pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y la firma de correos electrónicos.

El Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica además de la identificación del Suscriptor y de la Sociedad, contendrá información sobre la relación de representación que ostenta el suscriptor respecto de la Sociedad Representada, incluyendo un identificador único electrónico del Boletín Oficial del Estado que describa dicha representación, y que vincula al certificado con el Código de Validación Electrónica (CVE) del documento presentado.

1.6.4.2.4 Certificado Cualificado de Cargo Administrativo

Los Certificados Cualificados de Cargo Administrativo acreditan la identidad de su titular, así como su condición de funcionario perteneciente a la Administración del Estado o autonómica. Se emiten para su exclusivo uso en el ámbito de su actividad funcionarial y su relación con los Registros a través de los servicios interactivos suministrados por el CORPME. Se emiten para la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Cargo Administrativo pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y la firma de correos electrónicos.

Las firmas respaldadas por estos certificados acreditan la intervención personal del funcionario en todos los actos que son propios de su cargo, incluyendo las comunicaciones y la elaboración de todo tipo de documentos en formato electrónico.

Los Certificados Cualificados de Cargo Administrativo tienen como finalidad principal la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Cargo Administrativo también pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso.

1.6.4.2.5 Certificado Cualificado de Administración Local

Los Certificados Cualificados de Administración Local acreditan la identidad de su titular, así como su condición de funcionario o cargo perteneciente a la Administración Local. Se emiten para su exclusivo uso en el ámbito de su actividad funcionarial y su relación con los Registros. Se emiten para la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Administración Local pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y la firma de correos electrónicos.

Las firmas respaldadas por estos certificados acreditan la intervención personal del funcionario en todos los actos que son propios de su cargo, incluyendo las comunicaciones y la elaboración de todo tipo de documentos en formato electrónico.

Los Certificados Cualificados de Administración Local tienen como finalidad principal la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Administración Local también pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso.

1.6.4.2.6 Certificado Cualificado de Profesional

Los Certificados Cualificados de Profesional acreditan la identidad de su titular, y su pertenencia a una profesión regulada y sometida a la disciplina de un Colegio o Asociación Profesional. Su finalidad principal es la firma de los documentos que se presentan ante los Registros y Administraciones Públicas, y su uso en todas las comunicaciones que se realicen con éstos. Se emiten para la firma de documentos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido. Los Certificados Cualificados de Profesional pueden ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso y la firma de correos electrónicos.

En virtud de convenio específico entre el CORPME y los Colectivos Profesionales, podrá ampliarse el ámbito de uso de los certificados digitales del CORPME a fin de permitir su utilización en los actos propios de su giro o actividad. Sirviendo en tal caso, además de su función primaria, para garantizar la intervención del profesional en los negocios y procedimientos telemáticos en los que intervenga en dicha condición, incluyendo las comunicaciones y la elaboración de todo tipo de documentos en formato electrónico.

Los Certificados Cualificados de Profesional garantizan la identidad del emisor, el no repudio de origen y la integridad de contenido de documentos y comunicaciones. También podrán ser utilizados para asegurar la autenticación de su titular ante sistemas que lo requieran en un control de acceso.

1.6.5 Certificados de Componente

1.6.5.1 Certificado para Procedimientos Registrales

Los Certificados No Cualificados para Procedimientos Registrales respaldan las firmas realizadas de manera automática por los ordenadores de los Registros destinados a tal fin y, además, les permiten autenticarse ante los usuarios, así como establecer cifrados de sesión en las comunicaciones que realicen. Su titular será, en cada momento, el Registrador a cuyo cargo esté el Registro para el que han sido emitidos.

La función principal de estos certificados es permitir el envío de documentos electrónicos, que acrediten la recepción por el Registro de una firma o documento electrónico y el momento en que ésta se produjo (sello de tiempo).

1.6.5.2 Certificado No Cualificado de SSL genérico

Los Certificados No Cualificados de Servidor SSL vinculan los datos de verificación de Firma a una aplicación informática sobre un servidor con soporte SSL.

Sobre estos certificados, existirá un responsable que será una persona física que tendrá el control para actuar sobre el certificado.

La Unidad de Tramitación Central del CORPME emitirá estos certificados bajo solicitud aprobada según el procedimiento de gestión de solicitudes y validada esta solicitud por el Director Técnico del SSI del CORPME.

1.7 Limitación genérica de uso de los certificados

Los certificados digitales emitidos por el CORPME serán utilizados, única y exclusivamente para la finalidad para la que fueran emitidos, de conformidad con lo dispuesto en esta DPC, las PC's particulares y el Reglamento interno del PSC. Tal y como se ha señalado en el apartado anterior la limitación genérica de uso podrá ser modificada en virtud de los convenios que el CORPME suscriba con un determinado colectivo o asociación, a fin de amparar otros usos diferentes del primario autorizado.

Igualmente, los certificados deben emplearse únicamente de acuerdo con la legislación que le sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia de criptografía existentes en cada momento.

Los servicios de certificación que ofrece CORPME, no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como las relativas al funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otra donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

Cada PC establecerá las limitaciones específicas en el uso de sus certificados.

1.8 Definiciones y Acrónimos

1.8.1 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. A efectos de la presente Declaración de Prácticas de Certificación, son Autoridad de Certificación todas aquellas que en la misma se definan como tales.

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 Declaración de Prácticas de Certificación, cuando se haga referencia a Certificado se entenderá realizada a un Certificado emitidos por cualquier Autoridad de Certificación de CORPME.

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

Certificado 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 de CORPME puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de Prestador de Servicios de Certificación en cumplimiento de lo dispuesto por la Ley.

Dispositivo Seguro de Creación de Firma (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 Declaración de Prácticas de Certificación, se corresponderá con las Autoridades de Certificación pertenecientes a la jerarquía de CORPME.

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

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

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

PUK (Personal Unblocking Key): Número o clave específica sólo conocido por la persona que tiene que acceder a un recurso. 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 esta Declaración de Prácticas de Certificación.

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

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

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

1.8.2 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, Mercantiles y de Bienes Muebles de España.

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

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

CWA: CEN Workshop Agreement.

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

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).

1.9 Administración de la DPC

1.9.1 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.

1.9.2 Procedimiento de aprobación y modificación de la Declaración de Prácticas de Certificación

La aprobación y subsiguientes modificaciones de la DPC, 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 DPC 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 DPC, no otorgará al suscriptor ningún derecho a ser compensado por tal motivo.

1.10 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, Mercantiles y de Bienes Muebles 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

2 DIRECTORIO Y PUBLICACIÓN DE LOS CERTIFICADOS

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 Registro inicial

3.1.1 Tipos de nombres

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

3.1.2 Necesidad de que los nombres sean significativos

En todos los casos se recomienda que los nombres distintivos de los suscriptores de los certificados sean significativos.

En cualquier supuesto, el dotar a los nombres distintivos de significado viene dado por la política a tal efecto desarrollada y descrita en el documento de PC correspondiente al certificado en cuestión.

3.1.3 Reglas para interpretar 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 *"Certificate Policies. Policy Identifier"* debe ser único y no ambiguo.

Cada PC establecerá el mecanismo de unicidad de los nombres específico.

3.1.5 Procedimiento de resolución de conflictos

Según lo establecido en el apartado 9.13 del presente documento.

3.1.6 Reconocimiento, autenticación y papel de las marcas

No estipulado.

3.2 Validación inicial de la identidad

3.2.1 Medio de prueba de posesión de la clave privada

El par de claves es generado, por el dispositivo criptográfico seguro del solicitante y bajo su custodia, por lo que, la posesión de la clave privada correspondiente a la clave pública para la que el solicitante solicita que se genere el certificado, quedará probada mediante el envío de la petición de firma del certificado (CSR).

Este procedimiento podrá ser modificado por el que establezca en cada caso la PC aplicable.

3.2.2 Autenticación del solicitante cuando sea 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 Oficial del Registro 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 Oficial del Registro 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 Oficial de Registro debe comprobar que el CVE del Boletín Oficial del Estado (BOE) es accesible y refleja el nombramiento del solicitante.

3.2.3 Autenticación del solicitante cuando sea persona física

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 Oficial del Registro correspondiente solicitará la documentación acreditativa del atributo certificable de que se trate en virtud del tipo de certificado.

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

Si la inscripción correspondiente a los atributos es accesible a través de Internet, el Operador de la Unidad de Tramitación correspondiente deberá incluir en el certificado el código que permita el acceso directo a su contenido.

En el caso de los demás atributos el Operador de la Unidad de Tramitación correspondiente deberá realizar las comprobaciones documentales previstas en las correspondientes PC's, guardando copia de los documentos que éstas indiquen. También verificará la equivalencia entre los términos literales y plazo de los atributos documentados y su expresión en el certificado.

La pertenencia a Colectivos profesionales, es decir, Colegios o Asociaciones, se acreditará a los efectos de la expedición de Certificados Cualificados de Profesionales, mediante la aportación de Certificación suscrita por el Secretario del Colegio o Asociación al que esté adscrito el Solicitante, expedida un máximo de quince (15) días antes de la comparecencia en la Unidad de Tramitación correspondiente.

En virtud de convenio, el CORPME y el Colectivo Profesional interesado en obtener para sus miembros Certificados Cualificados de Profesionales, podrán establecer procedimientos de validación de atributos alternativos a la aportación de certificación del secretario del colectivo, señaladamente procedimientos técnicos de interconexión entre el CORPME y los repositorios del colectivo profesional, para la verificación en línea de la pertenencia del solicitante a dicho colectivo.

En la interconexión y acceso a los datos de colegiación del solicitante se adoptarán las medidas técnicas y de procedimiento, necesarias para la protección de los Datos de Carácter Personal de los Colegiados o Asociados incluidos en el Fichero automatizado de verificación.

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

En la PC correspondiente se describirá el procedimiento de la comprobación de las facultades de representación del solicitante.

3.2.6 Criterios para operar con CA externas

Para poder establecer relaciones de interactividad con CA's externas, el PSC del CORPME establecerá ciertos requisitos de seguridad para garantizar la adecuación de dichas CA's externas a la PKI del CORPME.

Los siguientes requisitos de seguridad definidos, podrán ser ampliados en cada caso por la AAP, según lo considere oportuno:

- La CA externa ha de proporcionar un nivel de seguridad en la gestión de los certificados, a lo largo de su ciclo de vida, como mínimo, igual al del PSC del CORPME. Esta exigencia se recogerá en la DPC y PC's correspondientes y en su cumplimiento por la CA.
- Deberá aportar el informe de auditoría de una Autoridad externa de reconocido prestigio relativa a sus operaciones como medio de verificación del nivel de seguridad existente. La AAP podrá declarar exentas de este requisito a la CA que estime oportuno.
- Establecer un convenio de colaboración en el que se fijen los compromisos adquiridos en materia de seguridad para los certificados incluidos en la interacción.

Del mismo modo, la AAP podrá denegar la solicitud de interactividad sin necesidad de aportar ninguna justificación, aunque la CA externa cumpla con los requisitos definidos anteriormente.

La interactividad puede llevarse a cabo mediante certificación cruzada, certificación unilateral u otras formas.

3.3 Identificación y autenticación para solicitudes de renovación

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

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

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

3.4 Identificación y autenticación para solicitudes de revocación

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

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

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

El proceso de emisión de los certificados digitales comienza con la Petición de cita y el alta del usuario en la agenda del CORPME: **https://www.registradores.org/scr/agenda**.

La generación del par de claves se realizará dentro de un dispositivo criptográfico seguro y con la intervención y custodia personal del solicitante del certificado, quien además introducirá por sí mismo las contraseñas de acceso a la clave privada.

4.1 Solicitud de certificados

4.1.1 Quién puede efectuar una solicitud

El solicitante objetivo varía en función del tipo de certificado cualificado. A continuación, se indica quién puede efectuar las solicitudes:

- Certificado Cualificado de Registrador: Registradores en activo.
- Certificado Cualificado para Personal Interno: Empleados del Colegio de Registradores, empleados de Registro, empleados del Decanato, cargos del Colegio de Registradores, cargos de la Junta de Gobierno del Colegio de Registradores, Registradores aspirantes, Registradores jubilados, Registradores excedentes y empleados de sociedades colegiales.
- Certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica: Decano-Presidente del Colegio de Registradores.
- Certificado Cualificado de Personal: Cualquier persona mayor de edad.
- Certificado Cualificado de Representante de Persona Jurídica: Cargos de entidades inscritas en los Registros Mercantiles.
- Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica: Registradores en activo.
- Certificado Cualificado de Profesional: Personal perteneciente a un colegio o asociación profesional con convenio con el prestador.
- Certificado Cualificado de Cargo Administrativo: Cargos de la administración pública.
- Certificado Cualificado de Administración Local: Personal adscrito a la administración local.

Adicionalmente, también podrá efectuar una solicitud de certificado el 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. En los siguientes apartados, se enumeran los certificados en función de dicha necesidad.

1. **Necesidad de solicitud de cita previa**

   Los certificados que requieren la solicitud mediante cita previa son los siguientes:

   - Certificado Cualificado de Personal.
   - Certificado Cualificado de Representante de Persona Jurídica.
   - Certificado Cualificado de Profesional.

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 Oficial de Registro a cargo de la Unidad de Tramitación, es imperativo que la comparecencia personal del solicitante coincida con la presencia del Registrador en la Unidad de Tramitación, por ello el solicitante deberá seleccionar día y hora, de entre los disponibles y previamente habilitados por el Oficial de la misma 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.

2. **No necesidad de solicitud de cita previa**

Los certificados que no requieren solicitud mediante cita previa son los siguientes:

- Certificado Cualificado de Registrador.
- Certificado Cualificado para Personal Interno.
- Certificado Cualificado de Representante de Entidad Jurídica para Facturación Electrónica.
- Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica.
- Certificado Cualificado de Cargo Administrativo.
- Certificado Cualificado de Administración Local.

En estos casos, se creará 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 certificados cualificados, se personarán con documento identificativo correspondiente y una certificación que acredite el cargo, y para las solicitudes de los Certificados No Cualificados la solicitud será mediante correo electrónico, y serán emitidos por la Unidad de Tramitación Central del CORPME.

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

En ambos supuestos, el solicitante se persona en la unidad de tramitación con el identificador de la cita, con el DNI, NIF, NIE, pasaporte u otro documento identificativo y la certificación que acredite el cargo, en los casos que correspondan. Dicho identificador, será entregado al Oficial de Registro quien lo introduce en el sistema, recuperando los datos introducidos en el apartado 3.2.3 del presente documento. De nuevo, se vuelven a hacer las comprobaciones de autenticación.

Con la comparecencia del usuario, en única instancia, ante la Unidad de Tramitación correspondiente se da paso, de ser positivo tras la verificación de identidad y atributos certificables, al proceso de emisión de certificados. Éste irá firmado por la CA a fin de establecer la cadena de confianza en la que se basa la firma electrónica.

Una vez realizado el trámite de identificación y, en su caso, el de comprobación de atributos del solicitante, el Oficial de Registro le transmitirá a éste la licencia de uso en formato electrónico. Posteriormente, el Oficial imprimirá dos copias de dicha licencia, las cuales deben ser firmadas por el mismo y el solicitante, quedando una copia en poder de cada uno de ellos.

La unidad donde se realizó la tramitación deberá conservar la licencia firmada durante un plazo de quince (15) años, a contar desde la caducidad o revocación del certificado.

Una vez validada la identidad del solicitante y los datos necesarios se procede a emitir el certificado solicitado.

4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

Para la autenticación de la persona física, tanto para nacionales como para extranjeros, y de la documentación acreditativa del atributo certificable de que se trate en virtud del tipo de certificado, se seguirá el procedimiento recogido en el apartado 3.2.3 del presente documento.

4.2.2 Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que el PSC del CORPME haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación.

El PSC del CORPME puede negarse a emitir un certificado a cualquier solicitante basándose exclusivamente en su propio criterio y salvaguardando, en cualquier caso, el principio de no discriminación, sin que ello implique contraer responsabilidad alguna por las consecuencias que pudieran derivarse de tal negativa.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

La CA del PSC del CORPME no se hacen responsables de las demoras que puedan surgir en el período comprendido entre la solicitud del certificado y la entrega del mismo. En todo caso, al ser requerida la realización de la cita previa para la emisión del certificado, no se esperan demoras en la tramitación de las solicitudes de los certificados, salvo aquellas producidas por incidentes técnicos ajenos al normal funcionamiento del PSC del CORPME.

4.3 Procedimiento de emisión de certificados

4.3.1 Actuaciones de la CA durante la emisión del certificado

Superados los trámites anteriores se procederá a la generación de las claves y, en su caso, a la emisión del certificado solicitado.

Para la emisión de los certificados cualificados y la generación del par de claves se utilizarán dispositivos criptográficos seguros, dentro de los cuales se realizará de manera directa e inmediata, la generación del par de claves y las operaciones criptográficas de firma, de tal modo que todas las funcionalidades previstas en las PC's se efectúen sin que, en ningún caso, sea necesario transferir a un equipo externo la clave privada (datos de creación de firma), garantizándose al suscriptor de este modo 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.

Tanto los DSCF como los formatos de fichero utilizados en el proceso de emisión del certificado son conformes con los estándares PKCS (*Public-Key Cryptography Standards*) de RSA Data Security Inc.

En el caso de los DSCF, éstos serán conformes con las normas técnicas (CWA: CEN WORKSHOP AGREEMENTS) emanadas por el Comité Europeo de Normalización (CEN) de conformidad con lo dispuesto en la Directiva 1999/93 por la que se establece un marco comunitario para la Firma Electrónica. Las homologaciones de seguridad, se detallan a continuación:

- Common Criteria EAL4+, FIPS 140-2 y CC EAL4+ PP-SSCD.
- Compatible con especificaciones ISO 7816-1 a 4.

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

Las solicitudes de certificados incluyen el correo electrónico del interesado, por lo que se envía un email notificando al solicitante la emisión del certificado por parte de la CA. Este email incluirá un código, que permitirá al titular llevar a cabo la revocación del certificado de forma remota a través de una llamada telefónica.

Cuando alguna de las CA's de la PKI del CORPME emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, facilitará la consulta de los certificados emitidos para aquellas autoridades interesadas.

4.4 Aceptación de certificados

4.4.1 Mecanismo de aceptación del certificado

La aceptación del certificado es la acción mediante la cual su suscriptor da inicio a sus obligaciones respecto al PSC del CORPME.

El suscriptor del certificado debe aceptarlo mediante la firma de la licencia de uso. En ningún caso se considerará a una persona titular de un certificado antes de que haya firmado la correspondiente licencia y ésta se encuentre en poder de la Unidad de Tramitación correspondiente.

El contenido de la licencia de uso viene especificado en la correspondiente PC. En la licencia de uso, el firmante debe comprometerse de forma expresa a cumplir las obligaciones enumeradas a lo largo del documento y, además, aceptar:

- Que cada firma digital creada usando la clave privada correspondiente a la clave pública certificada es la Firma Electrónica del suscriptor.
- Que cada vez que el suscriptor utiliza su certificado para acceder a cualquier tipo de información dicho acceso ha sido realizado por él personalmente.
- Que el uso de la clave privada certificada es personal e intransferible, por lo que toda utilización que se haga de ella por terceras personas será bajo la responsabilidad y riesgo del suscriptor. El suscriptor declarará disponer del exclusivo control sobre los *Datos de creación de Firma* (clave privada) asociados a los *Datos de verificación de Firma (clave pública)* incluidos en el certificado emitido a su nombre por el CORPME.
- Que acepta las limitaciones de uso correspondientes a la clase de certificado de que se trate y, en todo caso, que no usará la clave privada correspondiente a la pública certificada con el fin de firmar certificados o listas de certificados revocados.
- Que está de acuerdo con los términos y condiciones contenidas en este documento y en las PC's correspondientes.
- Que todos los datos suministrados durante el alta de usuario y solicitud del certificado son enteramente veraces.
- Que el certificado será utilizado de estricta conformidad con la legalidad y con las condiciones establecidas en la DPC y en las PC's particulares que resulten aplicables en virtud del tipo de Certificado de que se trate.

4.4.2 Publicación del certificado

El PSC del CORPME no publicará los certificados personales emitidos en ningún directorio web, ya que todos los certificados cualificados son generados directamente dentro de un DSCF, y en ningún caso se expiden en soporte software. Los certificados de dispositivos serán generados tanto en dispositivos como en soporte software y no serán publicados tampoco en ningún directorio web.

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

Cuando alguna de la CA de la PKI del CORPME emita un certificado de acuerdo con una solicitud de certificación tramitada a través de una RA, facilitará la consulta de los certificados emitidos para aquellas autoridades interesadas.

4.5 Par de claves y uso del certificado

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

En cualquier caso, el titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la correspondiente PC y de acuerdo con lo establecido en los campos '*Key Usage*' y '*Extended Key Usage*' del certificado.

Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la DPC y PC, y sólo para lo que éstas establezcan.

Tras la expiración o revocación del certificado, el titular dejará de usar la clave privada.

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

Los terceros que confían sólo pueden depositar su confianza en los certificados de acuerdo con lo establecido en el campo '*Key Usage*' y '*Extended Key Usage*' del certificado.

Los terceros que confían han de realizar las operaciones de clave pública de manera adecuada para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los mecanismos establecidos en esta DPC y en la correspondiente PC.

Asimismo, se adhieren a las condiciones de uso establecidas en dichos documentos.

4.6 Renovación de certificados sin cambio de claves

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

Las renovaciones de los certificados realizadas en el ámbito de esta DPC se realizarán siempre con cambio de claves.

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 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

Los certificados digitales que emite el CORPME son susceptibles de renovación siempre y cuando sean con cambio de claves. Caducado o extinguido un certificado digital, por agotarse el periodo de vigencia del mismo o por concurrir alguna de las causas de extinción recogidas en la presente DPC, únicamente cabrá solicitar un nuevo certificado digital.

4.7.1 Circunstancias para la renovación de certificados con cambio de claves

A continuación, se enumeran las causas de una renovación de un certificado digital del CORPME:

- Expiración del periodo de validez del certificado.
- Que el certificado haya sufrido cambios de formato.

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

Están legitimados para solicitar la renovación de un certificado:

- El titular del certificado o suscriptor.
- El representante legal del suscriptor del certificado, debidamente autorizado.
- Cuando aplique, la persona distinta al suscriptor que ha solicitado previamente el certificado y que ostenta un cargo que le autoriza para realizar dicha solicitud.

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

La solicitud de renovación del certificado puede ser:

- **Presencial:** Se lleva a cabo del mismo modo que una revocación y una obtención de certificados de manera presencial, pero realizadas éstas de forma conjunta.
- **No presencial:** Se aplica a usuarios con un certificado activo, dentro del período de renovación definido como dos (2) meses antes de la fecha de caducidad del certificado. Únicamente se permitirá realizar la renovación no presencial una vez, la siguiente el usuario está obligado a renovar presencialmente su certificado, según dicta la normativa de Firma Electrónica. El titular del certificado recibirá, dos (2) meses antes de la fecha de caducidad del mismo, una notificación que contendrá un enlace a través del cual

podrá realizar el proceso de renovación de forma remota. Dicho enlace le llevará a una página web que le solicitará el certificado electrónico a renovar y, posteriormente, comprobará que el certificado cumple los supuestos de renovación. Si la renovación es autorizada, se procederá a realizar una revocación y una obtención de certificados, enviando las notificaciones pertinentes al titular. El proceso de renovación es inmediato. En el caso de renovación de forma remota, el titular aceptará de manera implícita la licencia de uso firmada en la expedición inicial del certificado.

4.7.4 Notificación de la renovación de un certificado al titular

Las notificaciones al titular del certificado asociadas al proceso renovación serán las mismas que las realizadas durante una revocación y una obtención de certificados. De este modo, se notificará en primera instancia una revocación del certificado vigente y, a continuación, una emisión del nuevo certificado.

El titular tendrá la obligación de comprobar si la revocación del certificado ha sido publicada en el Directorio de Listas de Revocación.

4.7.5 Forma de aceptación del certificado con cambio de claves

La aceptación del certificado se realizará por parte del titular según lo establecido en el apartado 4.5.1 del presente documento.

4.7.6 Publicación del certificado con cambio de claves por la CA

No estipulado.

4.7.7 Notificación de la renovación del certificado por la CA a otras Autoridades

No estipulado.

4.8 Modificación de los certificados

Los certificados digitales que emite el CORPME no son susceptibles de modificación. Cuando se requiera la modificación de algún dato contenido en los certificados, se procederá a su renovación con los datos corregidos.

Por un lado, las modificaciones de certificados derivadas de los siguientes motivos se tratarán como una renovación de forma presencial:

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

Por otro lado, se tratarán como renovaciones de forma remota las modificaciones de certificados derivadas de las siguientes causas:

- Cambio de longitud de las claves.
- Cambio del algoritmo de firma.

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 los certificados

La revocación de un certificado supone la pérdida de su eficacia, siendo sus consecuencias equivalentes a las de la caducidad. La revocación del certificado producirá efectos frente a terceros inmediatos a través de OCSP y desde el momento en que sea publicada la lista CRL que contenga la revocación.

4.9.1 Circunstancias para la revocación

A continuación se enumeran las causas de la revocación de un certificado digital del CORPME:

- Que así lo soliciten el suscriptor del certificado, o la persona legitimada para la solicitud del mismo, o el representado en los Certificados de Representante.
- Que el suscriptor del certificado cese en su destino en el caso de los certificados internos.
- Que se emita un nuevo certificado para el mismo suscriptor que haga referencia a atributos idénticos, en el caso de los certificados externos.
- Que se cancele o modifique una inscripción a la que se refiera el contenido de un certificado de atributos basado en una inscripción registral.
- Que se haya perdido o inutilizado el soporte en el que está contenida la clave privada correspondiente a la pública certificada.
- Que un tercero haya utilizado indebidamente la clave privada correspondiente a la pública certificada.
- Que la clave privada correspondiente a la pública certificada haya sido desvelada o haya podido verse comprometida por cualquier circunstancia.

- Que el suscriptor haya fallecido o haya sido incapacitado legalmente o, en su caso, que haya perdido, definitivamente o por plazo que supere el de vigencia del certificado, la condición o cargo en virtud del cual se emitió el certificado así como cuando, por cualquier causa, se extinga la persona jurídica a quien el cargo o apoderado suscriptor del certificado represente.
- Que la información contenida en el certificado o los datos aportados por el titular durante el trámite de registro, sean inexactos, ya fuere por error o falsedad inicial del suscriptor o por cambios sobrevenidos.
- Que el certificado haya sufrido cambios de formato.
- Que el suscriptor haya incumplido las disposiciones de la presente DPC o alguna de las PC's.
- Que así se disponga en una resolución administrativa o en un auto o sentencia o también, en el caso de los certificados internos, en un expediente disciplinario.

4.9.2 Quién puede solicitar la revocación

Están legitimados para solicitar la revocación del certificado:

- El titular del certificado o suscriptor.
- El representante legal del suscriptor del certificado, debidamente autorizado.
- La entidad representada por el suscriptor del Certificado Cualificado de Representante, a través de su órgano de gobierno.
- Cuando aplique, la persona distinta al suscriptor que ha solicitado previamente el certificado y que ostenta un cargo que le autoriza para realizar dicha solicitud.
- En los certificados de atributos basados en una inscripción registral, el Registrador que autorice la modificación o cancelación de esta.
- El Decano del CORPME, o aquel en el que delegue, el Director Técnico del SSI, o el Registrador responsable de la Unidad de Tramitación que autorizó la emisión del certificado, cuando tuvieran constancia de la existencia de alguna de las causas mencionadas en el punto anterior.
- La autoridad judicial o administrativa en virtud de una resolución motivada.

4.9.3 Procedimiento de solicitud de revocación

4.9.3.1 Revocación a instancias del suscriptor del certificado

En caso de solicitar la revocación el suscriptor del certificado, ésta se realizará de forma automática y bajo la única responsabilidad del propio suscriptor que la solicite.

La revocación puede hacerse de dos formas:

- **Forma presencial:** El titular podrá revocar el certificado personándose en la Unidad de Tramitación que emitió el certificado o, en caso de urgencia, en cualquier otra Unidad de Tramitación del CORPME. Una vez identificado el titular, el Oficial de Registro imprimirá una solicitud de revocación y, una vez que ésta sea firmada por ambos, ordenará inmediatamente la revocación del certificado. En todo caso, el titular deberá cumplimentar el formulario de solicitud con sus datos personales, indicando la causa de solicitud de revocación. La disponibilidad del servicio depende del horario y calendario laboral de cada una de las Unidades de Tramitación.
- **Forma remota:** El titular podrá revocar el certificado de forma remota mediante una llamada telefónica, o firmando una solicitud electrónica. Para el primero de los métodos, llamada al Servicio de Asistencia Telefónica, la revocación tendrá efecto en el acto, tras

las comprobaciones necesarias para garantizar la identidad del solicitante. Durante todo el proceso, la comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación. Dicho servicio, tiene una disponibilidad de 24 horas al día, los 365 días del año, y se presta a través del número de teléfono +34 912701771.

En primer lugar, se verificará la identidad del usuario que realiza la llamada, comprobando la información personal relativa al tipo de certificado y atributos del suscriptor.

Posteriormente, se acreditará la identidad mediante el código de revocación proporcionado al usuario durante la emisión del certificado.

Ante el olvido o la pérdida del código de revocación por parte del usuario, se volverá a enviar dicho código al correo proporcionado en el proceso de emisión del certificado y, de esta manera, se podrá continuar con el proceso de revocación.

En caso de que la identidad del usuario que realiza la llamada no corresponda con la información del firmante del certificado, se le indicará que no es posible realizar la revocación vía telefónica, y se tendrá que poner en contacto con el CORPME para proceder a realizar la revocación mediante otro método estipulado.

Para el segundo de los métodos, firma de una solicitud electrónica, la revocación también tendrá efecto en el acto. En este caso, la identificación del usuario, se llevará a cabo con un certificado cualificado vigente del propio usuario. Para llevar a cabo este tipo de revocación, el solicitante tendrá que acceder al enlace: http://pki.registradores.org/, descargar la solicitud electrónica, firmarla e enviarla al correo electrónico: *revocaciones@corpme.es*. Inmediatamente después, deberá ponerse en contacto telefónico con el Servicio de Asistencia Telefónica para confirmar la recepción y obtener por parte del PSC la confirmación de que se ha llevado a cabo correctamente el proceso.

4.9.3.2 Revocación por persona distinta del suscriptor titular

La persona que ocupe el cargo que legitime para la solicitud de un determinado tipo de certificado, o el representado en los Certificados Cualificados de Representante, podrá ordenar la revocación de éste.

Para ello, deberá enviar una solicitud firmada a la Unidad de Tramitación que autorizó la emisión del certificado. Una vez comprueba la capacidad de la persona para actuar en nombre del titular, la Unidad de Tramitación procederá a la revocación del certificado, bajo la única responsabilidad del solicitante de la revocación.

4.9.3.3 Revocación de oficio

Los certificados podrán ser revocados de oficio por la Unidad de Tramitación Central o por el Registrador a cargo de alguna de las Unidades de Tramitación cuando concurra alguna de las causas señaladas en el presente documento.

Las resoluciones administrativas y sentencias judiciales deberán ser ejecutadas, en los certificados internos, por la Junta de Gobierno que enviará a la Unidad de Tramitación Central la orden correspondiente y, en los certificados externos, por el Registrador responsable de la Unidad de Tramitación que autorizó la emisión del certificado.

Recibida la orden de revocación, la Unidad de Tramitación, central o provincial según corresponda, revocará inmediatamente el certificado indicando al titular del certificado el hecho y la causa de la revocación.

La Unidad de Tramitación guardará copia de la resolución administrativa, auto, sentencia, o documento en que se funde la orden de revocación de oficio.

4.9.3.4 Revocación por causa de urgencia

La Unidad de Tramitación Central podrá autorizar la revocación de un certificado por causa de urgencia, cuando sea requerida por alguna de las personas mencionadas en el presente documento.

Una vez comprobada la identidad del solicitante de la revocación podrá requerir a quien solicitó la revocación urgente para que justifique su solicitud, hasta satisfacer los requisitos exigidos por las PC's para la causa de revocación alegada. Si dicha justificación no fuera posible o si la revocación hubiera causado perjuicios a terceros, la responsabilidad recaerá únicamente sobre el solicitante de la revocación.

Esta revocación tendrá efecto en el acto, tras las comprobaciones necesarias para garantizar la identidad del solicitante. La revocación de un certificado supone su total pérdida de validez y la exención de responsabilidad del Servicio de Certificación por cualquier daño producido como consecuencia del uso del certificado revocado con posterioridad a su revocación.

4.9.4 Período de gracia de la solicitud de revocación

No existe un periodo de gracia contemplado ante una solicitud validada de revocación de un certificado. La revocación producirá efectos frente al solicitante desde el momento en que entregue la correspondiente solicitud a la Unidad de Tramitación y, frente a terceros, desde que sea publicada en el Directorio de Listas de Revocación.

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

Como norma general, las solicitudes de revocación tendrán efecto en el momento en el que se solicitan, siempre tras las comprobaciones necesarias para garantizar la identidad del solicitante.

En caso de producirse algún incidente excepcional que imposibilite la revocación inmediata de los certificados, se establece un tiempo máximo admisible para la tramitación de revocaciones de 24 horas.

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

Los terceros de buena fe deberán verificar con la debida diligencia, antes de depositar su confianza en un certificado del CORPME, la validez y vigencia de los certificados utilizando el servicio OCSP o accediendo a la última lista de certificados revocados (CRL).

4.9.7 Frecuencia de emisión de CRL

Los certificados revocados son incluidos en una lista de certificados revocados (CRL), la cual es actualizada tan pronto se produzca una nueva revocación, publicándose la nueva lista en menos de un (1) minuto desde la revocación producida, en las direcciones URL identificadas en el apartado 2.1 del presente documento.

La CRL publicada indica la información sobre la fecha y hora de la próxima emisión programada.

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

Independientemente de la ocurrencia de nuevas revocaciones, se emitirá una nueva lista de revocación (CRL) firmada digitalmente por el CORPME cada doce (12) horas en el caso de la CA Subordinadas, y un (1) año de la CA Raíz, sin perjuicio de la reemisión de una nueva lista con cada revocación practicada.

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

El servicio de comprobación de estado de certificados se mantendrá accesible y a disposición de usuarios y terceros de manera permanente, a fin de facilitar la verificación de la vigencia de los certificados.

Para garantizar la disponibilidad del servidor de Directorio de Validación de Certificados, así como del servicio OCSP, se han dispuesto sistemas redundantes y deslocalizados, configurados para minimizar cualquier eventual disrupción en el servicio.

4.9.10 Requisitos de comprobación en línea de revocación

Los terceros que confían que recurran a la Autoridad de Validación para la comprobación en línea de la revocación de un certificado, deberá disponer de software que sea capaz de operar con el protocolo OCSP.

4.9.11 Otras formas de divulgación de información de revocación disponibles

Las PC's admiten el uso de Puntos de Distribución de CRL's (CDP) como otra forma de divulgación de la información de revocación disponible.

4.9.12 Requisitos especiales de revocación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

4.9.13 Causas para la suspensión

El CORPME sólo contempla dos estados posibles para los certificados digitales que emite, pudiendo encontrase éstos vigentes o revocados.

Aquellos supuestos en los que la vigencia del certificado quede en entredicho por circunstancias sobrevenidas a la emisión, se procederá a una revocación cautelar de oficio del certificado, de conformidad con lo dispuesto en el apartado correspondiente de la presente DPC.

La revocación de oficio realizada en los casos apuntados, no otorgará al Suscriptor derecho a otra compensación diferente de la exención de los costes asociados a la emisión de un nuevo certificado digital de la misma clase que el revocado.

En la emisión del nuevo certificado, se observarán en todo caso las mismas formalidades y procedimientos que con el certificado original revocado de oficio.

4.9.14 Quién puede solicitar la suspensión

No estipulado.

4.9.15 Procedimiento para la solicitud de suspensión

No estipulado.

4.9.16 Límites del período de suspensión

No estipulado.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

El PSC del CORPME dispone de dos (2) servicios que proporcionan información sobre el estado de los certificados emitidos por su CA:

- Publicación de las listas de revocación de certificados (CRL). El acceso a las CRL se realiza vía HTTP, en las direcciones publicadas en el apartado 2.1 del presente documento.
- Servicio de validación en línea (Autoridad de Validación, VA) que implementa el Online Certificate Status Protocol (OCSP) siguiendo la RFC6960. Mediante el uso de este protocolo es posible obtener el estado actual de un certificado electrónico sin requerir de las CRL consultándolo directamente a la VA.

4.10.2 Disponibilidad del servicio

El servicio, en sus dos variantes (CRL's y OCSP), está disponible de forma ininterrumpida todos los días del año, tanto para los terceros que confían como para los titulares de los certificados u otras partes que los requieran.

4.10.3 Características adicionales

El CORPME en ningún caso proporcionará un cliente OCSP para hacer uso del Servicio de validación en línea. Es responsabilidad de quien desee utilizar dicho servicio disponer de un cliente OCSP que cumpla la RFC6960.

4.11 Extinción de la validez de un certificado

Además de la extinción del certificado por el agotamiento del periodo de validez, los certificados del CORPME quedarán extinguidos en los supuestos siguientes:

- Fallecimiento del titular del Certificado.
- El titular, o responsable legal asignado, será el responsable de transmitir la pérdida de su capacidad o Inhabilitación del suscriptor, decretada judicialmente.
- En el caso de Certificados de Representante de Persona Jurídica: revocación de la representación orgánica o voluntaria, desde que ésta accede al Registro Mercantil; o pérdida de la personalidad jurídica de la Sociedad representada, por alguno de los supuestos legales de disolución o extinción societaria.
- Disolución o cese en la actividad de Prestador de Servicios de Certificación del CORPME.
- Resolución firme recaída en sede judicial o administrativa que ordene la revocación del certificado del suscriptor.
- Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

- Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado de manera que éste ya no fuera conforme a la realidad.
- Cualquier otra causa lícita prevista en esta DPC.

El CORPME informará al suscriptor acerca de esta circunstancia de manera previa o simultánea a la extinción o revocación de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

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

A fin de asegurar la confiabilidad y seguridad de sus operaciones como Prestador de Servicios de Certificación, el CORPME ha dispuesto e implantado controles de seguridad física y lógica en todas sus instalaciones, al igual que procedimientos de auditoría, tanto interna como independiente para el seguimiento y verificación del cumplimiento de las políticas, directivas y procedimientos en materia de seguridad.

5.1 Controles Físicos

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

La infraestructura técnica del CORPME se ubica en el Centro de Proceso de Datos (en adelante, CPD) del CORPME, dotado de las más estrictas medidas de seguridad física y de estrictos controles de acceso al edificio.

El acceso al CPD está estrictamente restringido y sólo el personal autorizado puede acceder a su interior, previa identificación de doble factor: tarjeta inteligente y huella digital, guardándose registro de todos los accesos a las instalaciones de proceso de datos.

Tanto el CPD como el resto de instalaciones y oficinas de la Sede del CORPME están permanentemente monitorizados desde de un control de seguridad con circuito de video vigilancia cerrado, detectores de movimiento y guardias de seguridad que patrullan día y noche las dependencias colegiales.

Se han definido zonas con distintos niveles de acceso y seguridad, no siendo posible acceder a determinadas áreas sin una autorización expresa que quedará reflejada en el correspondiente “Log” de accesos.

5.1.2 Acceso físico

Se dispone de un completo sistema de control de acceso físico de personas que conforman varios niveles de control. Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios humanos y técnicos.

5.1.3 Suministro eléctrico y acondicionamiento ambiental de las instalaciones del CORPME

La infraestructura técnica del CORPME tiene asegurada la continuidad de sus operaciones en caso de cortes en el suministro, mediante la utilización de sistemas de alimentación ininterrumpida de alta capacidad y una doble acometida eléctrica con dos proveedores de energía distintos.

A fin de garantizar el correcto funcionamiento de los equipos de proceso de datos, las dependencias del Centro de proceso de datos cuentan con equipos de aire acondicionado que mantienen la temperatura de operación de los sistemas siempre dentro de los parámetros óptimos.

5.1.4 Exposición al agua

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado que conforman el PSC del CORPME.

5.1.5 Medidas contra incendios e inundaciones

Las instalaciones del CORPME disponen de sistemas avanzados de detección y extinción de incendios, estando también acondicionadas para garantizar la estanqueidad de las salas que contienen el equipamiento de proceso de datos frente a inundaciones accidentales o catastróficas.

5.1.6 Sistema de almacenamiento

La información relacionada con el PSC del CORPME se dispone en medios de almacenamiento de forma segura. Los sistemas de almacenamiento se encuentran duplicados y balanceados, y están ubicados en diferentes localizaciones, de manera asíncrona, para eliminar el riesgo asociado a una única ubicación.

5.1.7 Eliminación de residuos

El CORPME dispone de una política de gestión de residuos que garantiza la destrucción de cualquier material que pudiera contener información relacionada con su PSC, así como una política de gestión de los soportes removibles que utiliza.

5.1.8 Política de Respaldo de Información

El CORPME ha definido políticas detalladas para la realización de las copias de respaldo relacionada con su PKI, y para la conservación de los soportes de información respaldada, diferenciando tres métodos de respaldo de la información atendiendo a los diferentes activos del PSC del CORPME.

En el almacenamiento interno y externo de la información de respaldo, se aplican todas las medidas legales y reglamentarias en materia de protección de datos.

5.2 Controles de procedimiento

Por razones de seguridad, la información relativa a los controles de procedimiento se considera información confidencial y sólo se incluye una parte de la misma.

El PSC del CORPME procura que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorías periódicas como queda recogido en el apartado 8 del presente documento.

Por otra parte, el PSC vela por el cumplimiento de la normativa para evitar cualquier situación que pudiera desembocar en un conflicto de interés y, de esta manera, no perjudicar la imparcialidad de las operaciones.

En lo relativo a la subcontratación de actividades dentro de los servicios de certificación, éstas se desarrollan según lo establecido en las Políticas y Prácticas de Certificación y en los contratos formalizados con las entidades.

Adicionalmente, cabe destacar que el PSC posee una Política de Seguridad de la Información que ha sido definida y aprobada por la Junta de Gobierno. En esta política se establece el marco de organización de seguridad y, para ello, se revisa el cumplimiento de los procedimientos operativos y controles relacionados con la seguridad en las instalaciones, los sistemas y los activos informativos que proporcionan los servicios.

Asimismo, se ha diseñado una segregación de funciones para evitar el control total de la infraestructura del PSC del CORPME por parte de una sola persona.

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

La definición y aceptación de los roles responsables de servicios de certificación es llevada a cabo por la Comisión Directora, garantizando el principio de "privilegio mínimo".

5.2.1.1 Roles de gestión de los módulos de seguridad hardware (HSM)

- **Administrador del HSM:** Tiene las facultades de realizar operaciones de administración sobre el HSM, como son la creación y la sustitución de un conjunto de tarjetas. Además es el único capacitado para llevar a cabo la autorización FIPS140-2 Nivel III requerida para operaciones de nivel crítico establecidas en la norma.
- **Operador del HSM:** Tiene la facultad de activar (cargar) las claves críticas de la PKI. La activación de las claves para su utilización está protegida por un conjunto de tarjetas criptográficas (diferente al de administrador del HSM).

5.2.1.2 Roles de gestión de la PKI del CORPME

Se distinguen los siguientes responsables para el control y gestión del sistema:

- **Administrador de Sistemas**: Responsable del funcionamiento de los sistemas que componen la PKI, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de datos, del repositorio de información y de los sistemas operativos.
- **Auditores de Sistemas:** Autorizados para consultar y monitorizar los archivos de actividad (logs) de los sistemas.
- **Administrador de Seguridad**: Responsables de la gestión e implementación de las Políticas y Prácticas de Seguridad, establecido en la presente DPC y en las PC's asociadas.
- **Administradores de Registro:** Responsables de la aprobación de emisión, suspensión y revocación de certificados.
- **Responsable del Registro**: Responsable de las tramitaciones de peticiones de los certificados y de la aceptación por sus suscriptores de las condiciones de uso.

5.2.2 Número de personas requeridas por tarea

Se requiere un mínimo de dos (2) personas, de un total de seis (6) personas, para realizar operaciones de administración sobre la PKI del CORPME, a excepción de las tareas de gestión de ciclo de vida de certificados de entidades finales, permitidas a un único Operador de Registro.

5.2.3 Roles que requieren segregación de funciones

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos (2) roles marcados como "incompatibles":

- Incompatibilidad entre el rol del Auditor de Sistema y cualquier otro rol.

- Incompatibilidad entre los roles administrativos (Administrador de Seguridad y Administrador de Sistemas; Administrador de Sistemas y Responsables de Registro).

5.3 Controles de personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Todo el personal que preste sus servicios en el ámbito del PSC del CORPME deberá poseer el conocimiento, experiencia y formación suficientes, para el mejor cometido de las funciones asignadas.

Para ello, el CORPME llevará a cabo los procesos de selección de personal que estime precisos con objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

Los requerimientos de cualificación y conocimiento necesarios también se aplican siempre que se realice una contratación de terceros para cualquiera de los servicios relativos al PSC.

5.3.2 Procedimientos de comprobación de antecedentes

Según los procedimientos de selección de personal establecidos por el CORPME.

5.3.3 Requerimientos de formación

Según los procedimientos establecidos por el CORPME.

En particular, el personal relacionado con la explotación del PSC, recibirá la formación necesaria para asegurar la correcta realización de sus funciones. Se incluyen en la formación los siguientes aspectos:

- Entrega de una copia de la DPC.
- Concienciación sobre la seguridad física, lógica y técnica.
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol.
- Procedimientos de operación y administración para cada rol.
- Procedimientos para la recuperación de la operación del PSC en caso de desastres.

5.3.4 Requerimientos y frecuencia de actualización de la formación

Según los procedimientos establecidos por el CORPME.

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6 Sanciones por actuaciones no autorizadas

Todos los puestos dentro del CORPME tienen claramente asignadas funciones y responsabilidades, así como requerimientos y controles de seguridad aplicables a cada función dentro la organización. Los requerimientos de seguridad habrán de ser firmados y aceptados por el trabajador, realizándose controles, tanto periódicos como aleatorios de su cumplimiento por parte del CORPME.

El incumplimiento, de las obligaciones específicas del empleado en materia de seguridad, dará lugar a las acciones disciplinarias procedentes, incluido el despido, además de las acciones civiles o penales a las que hubiere lugar atendidas la gravedad y reiteración de las infracciones.

El CORPME dispondrá una normativa interna en materia de seguridad, estableciendo mecanismos de control y disciplinarios para asegurar su estricto cumplimiento por parte de los empleados del servicio.

Entre otras obligaciones, las normas exigibles al personal contemplarán las siguientes:

- Prohibición de cualquier uso de los activos e instalaciones del CORPME para la realización de actividades ilegales, ilícitas o que atenten contra la moral y los derechos de terceros.
- Prohibición de disponer para usos ajenos a la actividad del empleado, de cualquier clase de información o documentación considerada sensible o confidencial, así como de transmitir hacia el exterior, o introducir dicha información en soportes de datos susceptibles de ser extraídos clandestinamente de las instalaciones del CORPME.
- Obligación de secreto y confidencialidad respecto de las informaciones a las que hubiera tenido acceso el trabajador en el desempeño de sus funciones, incluso después de finalizada la relación contractual.
- Prohibición absoluta de revelar a un tercero, incluso dentro de la propia organización, cualquier contraseña y demás datos de acceso necesarios para acceder a sistemas y aplicaciones del CORPME. El usuario que hiciera cesión de sus datos de acceso será personalmente responsable del uso que se haga de los mismos.
- Prohibición de cualquier intento de vulneración o ataque contra elementos o sistemas de seguridad, que tienda a la averiguación de claves de acceso, independientemente del método utilizado, o al copiado, edición o eliminación de programas, ficheros o informaciones contenidas en otros equipos situados dentro de la red corporativa, o fuera de ésta.
- Prohibición del abuso del correo electrónico corporativo en usos no relacionados con la actividad profesional, en particular el envío de correos masivos (SPAM) con finalidad comercial o publicitaria.
- Prohibición del uso abusivo de los recursos de red corporativos para finalidades no relacionadas directamente con la actividad laboral. En particular se prohíbe expresamente la utilización de programas de descarga de ficheros del tipo P2P (peer to peer).
- Prohibición de la instalación de cualquier software que no cuente con la correspondiente licencia de uso, y de la desinstalación no autorizada de software legal instalado en el equipo del empleado, y configurado por el personal del CORPME.
- Prohibición de acceder sin autorización, a cualquier clase de información sobre personas físicas o jurídicas, así como de incorporar datos personales sobre tales personas en ficheros automatizados sin autorización por escrito del CORPME. Se prohíbe asimismo la realización de cualquier tipo de tratamiento sobre los datos incorporados a los ficheros de datos de carácter personal, para elaborar perfiles de usuario que permitan inferir datos sensibles objeto de mayor protección que aquellos de los que se infieran.
- Observancia del procedimiento definido para la eliminación de residuos, borrado seguro de soportes de datos y destrucción de documentación obsoleta o incorrecta, cualquiera que sea su clase.
- Cesión en exclusiva al CORPME de cualesquiera derechos de propiedad intelectual, industrial y patentes, sobre los trabajos, programas, desarrollos, análisis, metodologías y en general cualquier producto derivado de la actividad del empleado constante la relación laboral.

5.3.7 Requisitos de contratación de terceros

Se aplicará la normativa general de las entidades del CORPME para las contrataciones.

5.3.8 Documentación proporcionada al personal

Se facilitará el acceso a la normativa de seguridad de obligado cumplimiento junto con la presente DPC y las contenidas en las PC's que sean de aplicación.

5.4 Procedimiento de auditoría de seguridad

5.4.1 Tipos de eventos registrados

El CORPME almacenará de manera automática información de seguimiento de eventos (logs) respecto de todas las operaciones relacionadas con los sistemas que dan soporte a su actividad de PSC. Se adoptarán medidas tendentes a asegurar la integridad de los registros de eventos, a fin de impedir que cualquier usuario trate de modificar o eliminar el rastro de las acciones realizadas en el sistema.

Entre la información de los eventos almacenados, se realiza un registro de las operaciones relativas a los DSCF, como son:

- Preparación de los dispositivos.
- Registro de información relevante (enviada o recibida) relacionada con el registro, generación, diseminación, revocación y gestión de dispositivos.

Para asegurar la detección y corrección de cualquier incidencia en los sistemas del CORPME, y la depuración de los errores y, en su caso, responsabilidades derivadas de uso, los logs del servicio serán objeto de una estricta política de copia de seguridad y custodia que asegure su conservación y disponibilidad a los fines indicados.

5.4.2 Frecuencia de procesado de registros de auditoría

Los registros se analizarán de manera manual cuando sea necesario, no existiendo una frecuencia definida para dicho proceso.

5.4.3 Periodo de conservación de los registros de auditoría

El CORPME archivará durante el periodo legalmente establecido, es decir, quince (15) años contados desde el momento de su expedición, cuantos documentos y datos sean precisos para el desarrollo de su actividad como PSC, de manera que puedan verificarse las operaciones efectuadas con los mismos.

Las licencias de uso, solicitudes de revocación, certificaciones acreditativas de atributos certificables, y en general cualesquiera documentos firmados de los que se deriven derechos y obligaciones para los intervinientes en el PSC del CORPME, se almacenarán durante un periodo mínimo de quince (15) años.

5.4.4 Protección de los registros de auditoría

Para el archivo de los documentos electrónicos se dispondrán todas las medidas necesarias para asegurar la confidencialidad de los datos personales, la protección contra accesos no autorizados, y mecanismos que aseguren la integridad y ausencia de alteraciones en la documentación almacenada.

Periódicamente se realizarán copias de respaldo del archivo electrónico en soportes removibles que se almacenarán en instalaciones de seguridad del CORPME, a fin de garantizar la recuperación de los datos del archivo en caso de desastre.

Los eventos registrados están protegidos mediante cifrado, de forma que nadie, salvo las propias aplicaciones de visualización de eventos, con su debido control de accesos, pueda acceder a ellos.

Los servicios de registro proporcionados por proveedores externos contratados por el PSC del CORPME utilizan los datos de registro, autenticando previamente su identidad para intercambiar de manera segura la información y, de esta manera, garantizar el cumplimiento de los requisitos de generales de seguridad y privacidad.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Las copias de respaldo de los registros de auditoría se realizan según las medidas estándar establecidas por el CORPME.

5.4.6 Notificación al sujeto causa del evento

No se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento.

5.4.7 Análisis de vulnerabilidades

La tecnología KeyOne de Safelayer dispone de mecanismos de comprobación de la integridad de los ficheros binarios y de funcionamiento de los sistemas de gestión de certificados.

5.5 Archivado de registros

5.5.1 Tipo de eventos archivados

El CORPME mantendrá un archivo con los siguientes documentos y ficheros relacionados con su actividad de Prestador de Servicios de Certificación.

- Documentación relativa a los protocolos de generación y conservación de las Claves Principales del Servicio: Raíz y de Autoridades de Certificación Interna y Externa.
- Lista de certificados digitales revocados (CRL's y ARL's).
- Logs y registros de incidencias de servicio.
- Solicitudes de emisión, revocación y licencias de uso de certificados.
- Documentación acreditativa de los atributos certificables.
- Histórico de versiones de la DPC y de las PC's.

5.5.2 Periodo de conservación de registros

El CORPME archivará durante el periodo legalmente establecido, es decir, quince (15) años contados desde el momento de su expedición, cuantos documentos y datos sean precisos para el desarrollo de su actividad como Prestador de Servicios de Certificación de manera que puedan verificarse las operaciones efectuadas con los mismos.

5.5.3 Protección del archivo

Los archivos de registro están protegidos mediante cifrado, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.

5.5.4 Procedimientos de copia de respaldo del archivo

Las copias de respaldo de los archivos se realizan según el procedimiento interno asociado del CORPME.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de información empleados por el PSC del CORPME garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de fuente segura del ROA que constata la fecha y hora. Todos los sistemas se sincronizan con esta fuente oficial.

El periodo de sincronización con UTC de eventos significativos del entorno, gestión de claves y servicios de revocación está definido en un intervalo de 24 horas.

5.5.6 Sistema de archivo de información (interno vs externo)

El sistema de recopilación de información de auditoría del PSC es una combinación de procesos automáticos y manuales ejecutados por las aplicaciones disponibles.

5.5.7 Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos contra manipulaciones no autorizadas. Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras tareas según corresponda.

5.6 Cambio de claves

Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de CA a los suscriptores y terceros aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el repositorio del PSC del CORPME.

5.7 Recuperación ante compromiso de clave o catástrofe

El PSC del CORPME ha desarrollado y aprobado un Plan de Continuidad de Negocio que contempla el procedimiento de actuación ante una vulnerabilidad de los datos de creación de firma, orientado a solventar el incidente con la mayor brevedad posible. Este procedimiento se basa en la realización de una serie de acciones para la gestión de la crisis como parte integrante del plan:

- Detener la prestación del servicio afectado.
- Revocar los certificados afectados.
- Ejecutar las comunicaciones pertinentes a las partes afectadas, incluyendo información sobre el compromiso producido.
- Estudiar la necesidad de activar el Plan de Terminación de las actividades del PSC.

5.7.1 Procedimientos de gestión de incidentes y compromisos

El CORPME tiene establecido un plan de seguridad que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios del PSC del CORPME.

En el caso de que se produjera un compromiso de los datos de verificación de firma de alguna Autoridad de Certificación, el CORPME informará a todos los titulares de certificados del CORPME y terceros aceptantes conocidos que todos los certificados y listas de revocación firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio.

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

Si los recursos hardware, software, y/o datos se alteran o se sospecha que han sido alterados se detendrá el funcionamiento del PSC hasta que se reestablezca la seguridad del entorno con la incorporación de nuevos componentes cuya adecuación pueda acreditarse. De forma simultánea se realizará una auditoría para identificar la causa de la alteración y asegurar su no reproducción.

Ante la pérdida de calibración de un reloj con el UTC, se procederá a la recuperación del servicio de sellado de tiempo a la mayor brevedad, según lo establecido en el Plan de Continuidad.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

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

En el caso de compromiso de la clave privada de la CA se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente CRL, cesando el funcionamiento de actividad de la CA y se procederá a la generación, certificación y puesta en marcha de una nueva Autoridad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso de la CA, el certificado revocado de la misma permanecerá accesible en el repositorio del PSC del CORPME con objeto de continuar verificando los certificados emitidos durante su periodo de funcionamiento.

Se notificará a todas los afectados que los certificados y la información sobre su revocación, suministrada con la clave comprometida de la CA, deja de ser válida desde el momento de la notificación, debiendo utilizar para verificar la validez de la información la nueva clave pública de la CA.

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

El sistema de Autoridades de Certificación del PSC del CORPME puede ser reconstruido en caso de desastre. Para llevar a cabo esta reconstrucción es necesario contar con:

- Un sistema con hardware, software y dispositivo Hardware Criptográfico de Seguridad similar al existente con anterioridad al desastre.
- Las tarjetas de administrador de la CA.
- Una copia de respaldo de los discos del sistema anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la CA, incluidas sus claves privadas.

Las copias de respaldo se realizan periódicamente y las funciones de copia de seguridad y restauración son llevadas a cabo por los roles responsables, aplicando los controles necesarios para asegurar la recuperación de la información esencial y del software.

El almacenado, tanto de las tarjetas de acceso de los administradores de la CA como de las copias de los discos de sistema de la CA, se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

5.8 Cese de una CA o RA

El CORPME cesará su actividad como PSC, en virtud del acuerdo de disolución adoptado por la Asamblea de Decanos Territoriales y Autonómicos, por una ley que así lo establezca o por resolución judicial firme.

5.8.1 Cese de una CA

En caso de terminación de una CA, el CORPME:

- Se asegurará de que los potenciales problemas para los suscriptores y los terceros aceptantes sean los mínimos, así como el mantenimiento de los registros requeridos para proporcionar prueba veraz del servicio de certificación a efectos legales.
- Comunicará cualquier circunstancia relevante que pueda impedir la continuación de su actividad de la CA.
- Notificará su intención de cese de actividad de CA como PSC a los titulares de sus certificados, usuarios o cualquier entidad con la que mantenga alguna relación contractual de uso de sus certificados, por cualquier medio que garantice el envío y la recepción de la notificación y con un plazo mínimo de antelación de dos (2) meses, o el periodo que establezca la legislación vigente.
- Mantendrá los certificados activos, así como el sistema de verificación (Autoridad de Validación) y revocación hasta la extinción de todos los certificados emitidos.
- Tramitará la revocación de los certificados de las CA's afectadas.
- Destruirá o deshabilitará las claves privadas de las CA's, incluidas sus copias de seguridad, de tal manera que no puedan ser recuperadas.
- Remitirá al Ministerio de Energía, Turismo y Agenda Digital con carácter previo al cese definitivo de su actividad la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia.

En caso de transferencia de la actividad a otra CA, el CORPME:

- Enviará los acuerdos de transferencia y un documento explicativo de las condiciones que regularán las relaciones entre el suscriptor y el PSC al cual se transfieren los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de dos (2) meses al cese de su actividad, o el periodo que establezca la legislación vigente.
- Transferirá, con el consentimiento expreso de los suscriptores y con estricta observancia de todas las garantías en materia de protección de datos personales, aquellos certificados que sigan siendo válidos en la fecha efectiva de cese de actividad, así como los derechos y obligaciones que se deriven de los mismos y la información y documentación relativa a todos los certificados emitidos, a otro PSC que garantice análogos niveles de seguridad y fiabilidad en sus procedimientos.
- Revocará los certificados transcurrido el plazo de dos (2) meses, o el periodo que establezca la legislación vigente, siempre que no exista un acuerdo de transferencia o sin el consentimiento expreso de transferencia por parte del suscriptor, que además debe aceptar las condiciones del PSC al que se transfieren.
- Transferirá todas las bases de datos importantes, archivos, documentos, registros de eventos y auditoría, certificados y claves empleadas a la entidad designada durante las 24 horas siguientes a su terminación, o el periodo que establezca la legislación vigente.

5.8.2 Cese de una RA

En caso de cese de una RA, el CORPME:

- Transferirá a la entidad designada, durante las 24 horas siguientes al cese, los registros que mantengan mientras exista la obligación de mantener archivada la información. De no ser así, los registros serán destruidos.

Realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios que confían.

6 CONTROLES DE SEGURIDAD TÉCNICA

Adicionalmente a los controles de seguridad física establecidos en las instalaciones del CORPME, y de las medidas de seguridad implantadas para la protección de los datos utilizados para la Prestación del Servicio de Certificación, el CORPME someterá su actividad a los más estrictos controles de seguridad técnica que aseguren el cumplimiento de los más elevados estándares de calidad y fiabilidad, de conformidad con la normativa de aplicación y los estándares técnicos y de mercado.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Tanto el Certificado Raíz como las claves secundarias de las autoridades de certificación Interna y Externa del CORPME, se han generado siguiendo los procedimientos y formalidades definidos en la Ceremonia de Claves previa al inicio de la actividad del PSC, con intervención personal del Director del Servicio, y la presencia de miembros de la Junta de Gobierno en calidad de testigos del acto de generación.

Las Claves del Servicio han sido generadas directamente en el interior de un dispositivo criptográfico seguro, certificado como FIPS 140-2 de nivel 3, utilizando algoritmos RSA con una longitud de clave de 2048 bits, y de 4096 bits en caso de la CA Raíz y Subordinadas.

La custodia de los datos de creación de firma de la CA Raíz y Subordinadas corresponde al Director del Servicio, encontrándose el dispositivo contenedor de las claves en una caja fuerte de alta seguridad.

El periodo de vigencia para las claves del servicio se ha restringido por motivos de seguridad a un máximo de doce (12) años, aun cuando los estándares permiten una vigencia superior que podrá llegar a veinte (20) años.

El CORPME, una vez agotado el periodo de validez de las Claves del Servicio (Raíz y Secundarias), almacenará de manera segura las mismas, a fin de impedir su ulterior utilización. Procediendo, de conformidad con los protocolos definidos para la Ceremonia de Claves, a la generación de unas nuevas claves del Servicio.

Los pares de claves para el resto de titulares se generan en función de lo estipulado en la PC aplicable a cada certificado.

Los dispositivos hardware o software a utilizar en la generación de claves para cada tipo de certificado emitido por el PSC del CORPME vienen definidos por la PC que le sea de aplicación.

6.1.2 Entrega de la clave privada al titular

La clave privada de los certificados es generada por el propio titular en su dispositivo criptográfico, por lo que, en ningún caso, la distribución del dispositivo y la generación de la clave privada suponen un riesgo de seguridad relativo a la propia entrega.

El dispositivo criptográfico de creación de firma se almacena de forma segura y se distribuye directamente al titular para evitar posibles incidentes en el envío y la recepción.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública de los certificados es generada en el propio dispositivo criptográfico seguro del titular.

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

Tanto la Clave Principal o Raíz del Servicio, como las correspondientes a las autoridades de certificación subordinadas de la Clave Secundaria de Internos y Externos, estarán permanentemente disponibles para su descarga desde la página Web del portal del CORPME (**http://pki.registradores.org/normativa/index.htm**).

6.1.5 Tamaño de las claves

El tamaño de las claves utilizadas es:

- 4096 bits para la Autoridad Certificadora raíz del CORPME.
- 4096 bits para la CA de Certificados Internos y Certificados Externos.
- 2048 bits para la Autoridad de Sellado de Tiempo.

El tamaño de las claves para cada tipo de certificado emitido por el PSC del CORPME viene definido por la PC que le sea de aplicación.

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

El periodo de utilización de la clave privada será en general el mismo que el de vigencia del certificado. No obstante lo anterior, y con reflejo en la PC correspondiente, podrá establecerse mediante la introducción de una extensión dentro del estándar X509 v.3, un periodo de uso de la clave privada más reducido que el de vigencia del certificado, en aquellos casos en que la representación o atributo certificado ostentado por el suscriptor tenga un vencimiento conocido y anterior a la caducidad del propio certificado. En estos casos, el periodo de vigencia del certificado se limitará al de validez del mismo, es decir, al de la vigencia del atributo representado.

6.1.7 Usos admitidos de la clave (campo *KeyUsage* de X509 v3)

Los usos admitidos de la clave para cada tipo de certificado emitido por el PSC del CORPME vienen definidos por la PC que le sea de aplicación.

Todos los certificados emitidos por el PSC del CORPME contienen la extensión Key Usage definida por el estándar X.509 v3, la cual se califica como crítica. Se podrán establecer limitaciones adicionales mediante la extensión Extended Key Usage.

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

6.2.1 Estándares para los módulos criptográficos

Los módulos criptográficos utilizados en el PSC del CORPME para para la creación de claves utilizadas, cumplen con la certificación FIPS 140-2 de nivel 3.

La puesta en marcha de cada una de las Autoridades de Certificación, conlleva las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las claves de los
  - Administradores del HSM
  - Operadores del HSM
  - Administradores de seguridad

- Administrador de sistemas
- Administradores de registro
- Auditores de sistemas

- Generación de las claves de la CA.

El PSC del CORPME utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros.

6.2.2 Control multipersona (K de N) de la clave privada

La clave privada de las CA's del PSC del CORPME se encuentra bajo control multipersona. Ésta se activa únicamente mediante la inicialización del software de CA por medio de la combinación mínima de los operadores de la CA correspondientes.

Son necesarios dos (2) Administradores de los HSM del CORPME, de un total de seis (6), para permitir posteriormente que uno (1) de los cinco (5) Operadores del HSM puedan activar y usar la clave privada de la CA's.

6.2.3 Custodia de la clave privada

Las claves privadas de las Autoridades de Certificación que componen el PSC del CORPME se encuentran alojadas en dispositivos de hardware criptográfico seguro, y disponen de la certificación FIPS-2 de nivel 3 asociadas a las distintas CA's, utilizando algoritmos RSA con una longitud de clave de:

- 4096 bits para las CA Subordinadas.
- 4096 bits para la CA Raíz.

6.2.4 Copia de seguridad de la clave privada

Las claves privadas de las CA's del PSC del CORPME están archivadas en dispositivos criptográficos seguros, con características similares a las de los HSM y a los que sólo los operadores de la CA Raíz tienen acceso.

6.2.5 Archivado de la clave privada

Las claves privadas de los usuarios nunca serán archivadas una finalice su periodo de validez para garantizar el no repudio.

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

La transferencia de la clave privada se realiza entre módulos criptográficos (HSM) y requiere de la intervención de, al menos, dos (2) de los seis (6) Administradores del HSM y uno (1) de los cinco (5) Operadores del HSM para su posterior activación.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en el módulo criptográfico seguro en el momento de la creación de cada una de las Autoridades del PSC del CORPME. Cada una de estas Autoridades hace uso de dichos módulos y se guardan cifradas.

Se garantiza la seguridad de la clave privada en el módulo criptográfico a través de medidas preventivas que evitan la manipulación del dispositivo almacenado.

6.2.8 Método de activación de la clave privada

Tal y como se recoge en el apartado 6.2.2 del presente documento, la clave privada de las CA's del PSC del CORPME, se activa mediante la inicialización del software de CA por medio de la combinación mínima de los operadores de la CA correspondientes (Administradores y Operadores).

Concretamente, son necesarios dos (2) Administradores de HSM de la PKI del CORPME, de un total de seis (6), para permitir posteriormente que uno (1) de los cinco (5) Operadores del HSM puedan activar y usar la clave privada de la CA's.

6.2.9 Método de desactivación de la clave privada

Los Administradores del HSM, en combinación con los Operadores del HSM pueden proceder a la desactivación de la clave de las Autoridades de Certificación del PSC del CORPME mediante la parada de la aplicación informática de la CA correspondiente.

6.2.10 Método de destrucción de la clave privada

No estipulado.

6.2.11 Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados se encuentran certificados y cumplen con 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

Los *Datos de verificación de Firma* de los *Suscriptores* permanecerán archivados por si fuera necesaria su recuperación, en archivos y soportes seguros tanto física como lógicamente, durante el período legalmente establecido de quince (15) años.

6.3.2 Períodos operativos de los certificados y período de uso para el par de claves

El certificado y el par de claves de la Autoridad Certificadora del CORPME tienen una validez de veinticuatro (24) años y los de la CA de Certificados Externos y CA de Certificados Internos de doce (12) años.

El periodo de validez del resto de certificados vendrá establecido por la PC que corresponda.

6.4 Datos de Activación

6.4.1 Generación e instalación de los datos de activación

Para la creación de la Autoridad de Certificación se deben crear tarjetas criptográficas, que servirán para actividades de recuperación y funcionamiento. A continuación se detallan los roles utilizados en la CA del CORPME, cada uno con sus correspondientes tarjetas criptográficas:

- Tarjetas de Administrador del HSM.

- Tarjetas de Operador del HSM.
- Tarjetas de Administradores de Seguridad.
- Tarjetas de Administrador de Sistemas.
- Tarjetas de Auditores del Sistema.
- Tarjetas de Administradores de Registros.

Si una o más tarjetas se pierden o dañan, o el administrador olvida su PIN o dejan de ser utilizables por alguna razón, deberá volverse a generar todo el conjunto de tarjetas tan pronto como sea posible utilizando la totalidad de tarjetas de seguridad repartidas.

6.4.2 Protección de los datos de activación

Sólo el personal autorizado, en este caso los operadores de la partición correspondientes a cada CA, posee las tarjetas criptográficas con capacidad de activación de la CA y conoce los PIN y contraseñas para acceder a los datos de activación.

Al establecerse control multipersona, sin la intervención previa de los Administradores del HSM, los Operadores del HSM no podrán llevar a cabo la activación de la CA por sí mismos.

6.4.3 Otros aspectos de los datos de activación

No estipulado.

6.5 Controles de Seguridad Informática

Los datos relativos a este apartado se consideran información confidencial y solo se proporcionarán a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

El PSC del CORPME aplica las medidas de seguridad informática relativas a:

- Seguridad perimetral y de red, para proteger los dominios de la red interna del PSC contra el acceso no autorizado. Se proporcionan servicios continuos de vigilancia y alarma para detectar, registrar y reaccionar oportunamente ante cualquier intento no autorizado de acceso a sus recursos.
- Gestión de usuarios, para gestionar el alta, baja y modificación de cuentas de usuario.
- Política de control de acceso, incluida la separación de funciones de administración y operación de la seguridad. La aplicación de difusión cumple el control de acceso en los intentos de agregar o eliminar certificados y modificar otra información asociada. La aplicación de estado de revocación impone el control de acceso en los intentos de modificar la información de estado de revocación.
- Identificación y autenticación de usuarios, para utilizar las aplicaciones críticas. Se aplica la autenticación multifactorial para todas las cuentas capaces de causar directamente la emisión de un certificado.

El CORPME mantiene los componentes de la red local del PSC en un entorno físicamente y lógicamente seguro, y las configuraciones de dichos componentes se revisan periódicamente para verificar el cumplimiento de los requisitos establecidos.

6.5.1 Requerimientos técnicos de seguridad específicos

Los datos relativos a este apartado se consideran información confidencial y solo se proporcionarán a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

6.5.2 Evaluación de la seguridad informática

El PSC del CORPME evalúa de forma periódica su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas o internas e inspecciones, así con la realización continua de controles de seguridad.

6.6 Controles de Seguridad del Ciclo de Vida

Los datos relativos a este apartado se consideran información confidencial y solo se proporcionarán a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

El PSC del CORPME aplica las medidas de seguridad del ciclo de vida relativas a:

- Gestión de cambios, para administrar nuevos proyectos, evolutivos y correcciones de software.
- Control de software malicioso, para proteger la integridad del sistema contra virus o software malicioso.
- Gestión de soportes, frente a la obsolescencia y el deterioro de los medios de almacenamiento.
- Control de actualizaciones y parches de seguridad, frente a vulnerabilidades en el sistema.

6.6.1 Controles de desarrollo de sistemas

Los datos relativos a este apartado se consideran información confidencial y solo se proporcionarán a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones. Estos controles son exigibles desde su inicio, tanto en la adquisición de sistemas informáticos, como en el desarrollo de los mismos.

6.6.2 Controles de gestión de seguridad

El PSC del CORPME mantiene un inventario de todos los activos informáticos y realiza su clasificación de acuerdo con las necesidades de protección que tiene definido, alineado con el análisis de riesgos que ha efectuado.

El PSC del CORPME realiza controles periódicos de las necesidades de capacidad. Debido a ello, se dispone de un Plan de Capacidad para monitorizar y proyectar los requerimientos futuros de capacidad de la infraestructura, asegurando un grado de disponibilidad y ocupación de los servicios, e identificando futuras inversiones para mantener la capacidad de procesamiento y almacenamiento de los servicios.

La configuración de los sistemas se audita de forma periódica.

6.6.3 Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas en el PSC del CORPME.

6.7 Controles de Seguridad de la Red

Los datos relativos a este apartado se consideran información confidencial y solo se proporcionarán a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

El PSC del CORPME realiza análisis de vulnerabilidades y test de penetración fiables en los sistemas para mejorar la seguridad.

Además, aplica las medidas de seguridad de la red relativas a:

- Segmentación de sus sistemas en redes, considerando la relación funcional, lógica y física entre sistemas y servicios. Se realiza un bastionado de los equipos de la CA, deshabilitando a todos aquellos usuarios, aplicaciones, servicios, protocolos y puertos que no se utilicen en las operaciones de dicha CA.
- Seguridad en las comunicaciones, mediante canales seguros lógicamente distintos de otros canales de comunicación. Se cuenta con procedimientos de seguridad para la protección de sistemas y comunicaciones, que mantienen los sistemas de la CA en una zona segura de red.
- Accesibilidad en zonas de alta seguridad, para el acceso único de los roles responsables.
- Disponibilidad de los servicios de red.

6.8 Sellado de Tiempo

El sellado de tiempo (Timestamping) es un mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo.

El CORPME es una Autoridad de Sellado de Tiempo (TSA o Timestamp Authority) que actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

La Política Sellado de Tiempo del Colegio de Registradores establecerá las obligaciones y responsabilidades, así como los requerimientos operacionales durante el sellado de tiempo.

7 PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 Perfil de Certificado

7.1.1 Número de versión

Todos los certificados que emite el CORPME son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

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*

Las PC's del PSC del CORPME pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

El PSC del CORPME tiene definida una política de asignación de OID dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados del CORPME comienza con el prefijo 1.3.6.1.4.1.17276.0.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

7.1.4 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).

7.1.5 Restricciones de los nombres

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

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

Cada una de las PC's definirá su propio identificado de objeto (OID).

El PSC del CORPME tiene definida una política de asignación de OID dentro de su rango privado de numeración por la cual el OID de todas las PC's del PSC del CORPME comienza con el prefijo 1.3.6.1.4.1.17276.0.

7.1.7 Uso de la extensión "PolicyConstraints"

No estipulado.

7.1.8 Sintaxis y semántica de los "PolicyQualifier"

La extensión Certificate Policies contiene los siguientes Policy Qualifiers:

- CPS: contiene la URL que recoge la DPC y las PC's que rigen el certificado.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

7.1.9 Tratamiento semántico para la extensión crítica "Certificate Policy"

Si se desea mantener la máxima capacidad de poder operar con otras CA del certificado, la extensión será clasificada como *nonCritical*. Esto se hace siguiendo las recomendaciones para aplicaciones estándar de correo electrónico seguro S/MIME [RFC5750] y autenticación web SSL/TLS [RFC5246]. Las aplicaciones pueden utilizar la información contenida en dicha extensión, aun siendo una extensión no crítica.

7.2 Perfil de CRL

7.2.1 Número de versión

El Directorio se publica de acuerdo con el estándar LDAP (Lightweight Directory Access Protocol) y las listas de certificados revocados según la norma correspondiente (Certificate Revocation List, versión 2) del estándar X.509. También podrá utilizarse el estándar OCSP (On line Certificate Status Protocol).

7.2.2 CRL y extensiones

No estipulado.

7.3 Perfil de OCSP

7.3.1 Número(s) de versión

Además de la publicación de las CRL's, el PSC 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. Las URL de acceso al servicio OCSP son las siguientes: **http://ocsp.registradores.org** y **https://ocsp.registradores.org**

7.3.2 Extensiones OCSP

La Autoridad de Validación soporta:

- Peticiones firmadas.
- Extensión NONCE.

8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia o circunstancias de los controles para cada Autoridad

Con carácter periódico y a fin de verificar la efectiva implantación de las medidas recogidas en la DPC y PC's, el Responsable de Seguridad ordenará y supervisará la realización de auditorías internas e independientes.

Adicionalmente, el PSC del CORPME podrá realizar auditorías a las diferentes Unidades de Tramitación, para garantizar el ciclo de vida de los certificados y supervisar los procedimientos asociados.

8.2 Identificación/Cualificación del Auditor

Las Auditorías Internas serán realizadas por personal propio cualificado, e independientes llevadas a cabo por expertos de reconocido prestigio.

8.3 Relación entre el Auditor y la Autoridad Auditada

Para evitar un conflicto de intereses, el auditor externo y la parte auditada no deberán tener relación alguna, al margen de la función de auditoría.

8.4 Aspectos cubiertos por los controles

La auditoría determinará la adecuación de los servicios del PSC del CORPME con esta DPC y las PC's aplicables. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

El ámbito de actividad de una auditoría incluirá, al menos a:

- Política de seguridad y privacidad
- Seguridad física
- Evaluación tecnológica
- Administración de los servicios de la CA
- Selección de personal
- DPC y PC's competentes
- Contratos

8.5 Acciones a tomar como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. La Autoridad de Aprobación de Políticas (AAP), en colaboración con el auditor, será la responsable de la determinación de las mismas.

En el caso de observarse deficiencias graves la Autoridad de Aprobación de Políticas podrá adoptar, entre otras, las siguientes decisiones: suspensión temporal de las operaciones hasta que las deficiencias se corrijan, revocación del certificado de la Autoridad, cambios en el personal implicado, invocación de la política de responsabilidades y auditorías globales más frecuentes.

8.6 Comunicación de resultados

Aunque el resultado de la misma tiene el carácter de información confidencial, las deficiencias detectadas en el desarrollo de dicha Auditoría serán subsanadas en el menor tiempo posible siempre que sean anomalías de CORPME.

9 OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

La expedición de los certificados de la clave externa se realizará de forma gratuita para todos los particulares que soliciten un certificado personal, al igual que para el resto de solicitantes de certificados de la clave externa.

Toda vez que por motivos de seguridad y a los efectos de configurar una Firma Electrónica cualificada, los certificados cualificados son generados directamente dentro de un DSCF, y en ningún caso se expiden en soporte software, el solicitante deberá obtener como requisito previo a la emisión de su certificado, y a sus expensas, un Dispositivo de Creación de firma homologado por el CORPME. En las Unidades de Tramitación existirán a disposición de los solicitantes interesados "*Kits de Firma Electrónica*" que incluyen un DSCF homologado, así como el software licenciado necesario para la utilización del certificado.

Las consultas relacionadas con el precio aplicable a los Kits de firma, y las condiciones para el pago del mismo, se atenderán bajo demanda en la que el interesado deberá dirigirse al CORPME a través de la dirección de correo electrónico: **psc@registradores.org**.

9.1.2 Tarifas de acceso a los certificados

Las consultas relacionadas con las tarifas de acceso a los certificados del PSC del CORPME, se atenderán bajo demanda en la que el interesado deberá dirigirse al CORPME a través de la dirección de correo electrónico: **psc@registradores.org**.

9.1.3 Tarifas de acceso a la información de estado o revocación

Las consultas relacionadas con las tarifas de acceso a la información de estado o revocación de los certificados del PSC del CORPME, se atenderán bajo demanda en la que el interesado deberá dirigirse al CORPME a través de la dirección de correo electrónico: **psc@registradores.org**.

9.1.4 Tarifas de otros servicios

Las consultas relacionadas con las tarifas de cualquier otro servicio del PSC del CORPME, se atenderán bajo demanda en la que el interesado deberá dirigirse al CORPME a través de la dirección de correo electrónico: **psc@registradores.org**.

9.1.5 Política de reembolso

Las consultas relacionadas con la política de reembolso del PSC del CORPME, se atenderán bajo demanda en la que el interesado deberá dirigirse al CORPME a través de la dirección de correo electrónico: **psc@registradores.org**.

9.2 Responsabilidades Económicas

El CORPME dispone de la solvencia financiera necesaria para hacer frente a las responsabilidades que la legislación vigente le obliga a asumir. Dichas responsabilidades se encuentran cubiertas mediante instrumentos de aseguramiento admitidas por la Ley 59/2003, por el importe legalmente establecido de TRES MILLONES DE EUROS (3.000.000 €).

Las PC's aplicables a cada tipo de certificado establecerán la cuantía máxima hasta la que se extenderá la responsabilidad por daños y perjuicios del CORPME frente a suscriptores y terceros.

9.2.1 Indemnización de la CA's y/o RA's

No estipulado.

9.2.2 Relaciones fiduciarias entre varias entidades

No estipulado.

9.2.3 Procedimientos administrativos

No estipulado.

9.3 Confidencialidad de la información

Con independencia de lo establecido en el artículo 6 del Real Decreto-Legislativo 1298/1986, de 26 de junio, sobre el deber de confidencialidad de los datos e informaciones de las que disponga el CORPME en el ejercicio de sus funciones, se establece el siguiente régimen de confidencialidad de los datos relativos al PSC del CORPME.

9.3.1 Ámbito de la información confidencial

Se considerará de carácter confidencial toda la información generada por el PSC del CORPME que no sea estipulada como publica. Queda determinada expresamente como información confidencial lo siguiente:

- Las claves privadas de las Autoridades que componen el PSC del CORPME.
- La información relativa a las operaciones que lleve a cabo el PSC del CORPME.
- La información referida a los parámetros de seguridad, control y procedimientos de auditoría.
- La información de carácter personal proporcionada por los suscriptores de certificados a el PSC del CORPME durante el proceso de registro, de conformidad con lo dispuesto en la normativa sobre protección de datos de carácter personal y reglas de desarrollo.

9.3.2 Información no confidencial

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en el presente documento.
- La incluida en las PC's que le sean de aplicación.
- Los certificados emitidos por el PSC del CORPME.
- La lista de los certificados suspendidos o revocados (CRL's).

9.3.3 Deber de secreto profesional

Quedan obligados al deber de secreto profesional todos los empleados del CORPME que participen en cualquiera de las tareas propias o derivadas de su PSC. El personal contratado que participe en cualquier actividad u operación del PSC del CORPME queda igualmente sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con el CORPME.

9.4 Protección de la información personal

9.4.1 Marco legal aplicable

La política del CORPME en materia de Protección de datos personales se desarrollará de conformidad con la normativa tanto nacional como comunitaria vigente en la materia:

- Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de noviembre, por el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

9.4.2 Protección de Datos aplicable a la actividad del CORPME

El CORPME, protegerá los Ficheros que contengan Datos de Carácter Personal de conformidad con lo dispuesto en la legislación vigente, en particular la LOPD 15/1999, y el Reglamento 1720/2007.

Salvo en lo relativo a los Certificados Cualificados de Registrador, y a los Certificados Cualificados de Representante de Persona Jurídica, en tanto que estos contengan información societaria publicable en el Registro Mercantil, los ficheros de datos utilizados en la gestión del servicio de certificación tendrán carácter privado. Los datos obrantes en los Registros Públicos y que en virtud de las PC's se incorporen a los certificados del CORPME, serán tratados de estricta conformidad con la política de Protección de Datos del Colegio de Registradores de España, titular de los Ficheros de Datos que contienen la información relativa a sociedades y sus representantes.

El CORPME será respecto de los datos contenidos en los ficheros públicos de información mercantil, responsable únicamente de su tratamiento, el cual se realizará de conformidad y con las garantías definidas en la legislación vigente.

La creación, alteración y destrucción de los ficheros que contengan datos de carácter personal será oportunamente notificada al Registro General de Protección de Datos, puesto a cargo de la Agencia Española de Protección de Datos.

La titularidad de los ficheros de datos de carácter personal recabados con ocasión de la prestación del Servicio de Certificación, serán de titularidad del CORPME quien procederá a su inscripción y mantenimiento de conformidad con el régimen aplicable.

Las Unidades de Registro situadas en los Registros Mercantiles y otros puntos de registro que el Colegio de Registradores pueda autorizar previo acuerdo de la Junta de Gobierno del CORPME, en cuanto tengan acceso a documentos y datos de carácter personal de los solicitantes y suscriptores de certificados, para la realización de sus funciones, ostentarán respecto de dichos datos la consideración de Responsables de su tratamiento, el cual de conformidad con el artículo 12 de la LOPD, a lo establecido a continuación. Además, las *Unidades de Tramitación*, en cumplimiento con lo establecido en los artículos 7, 9 y 12 de la LOPD se comprometen a:

- Acceder a los ficheros y datos de carácter personal cuya titularidad corresponda al CORPME, únicamente en la medida en que dichos datos sean necesarios para su actividad como Autoridad de Registro, y en consecuencia darles el uso que corresponda excluyendo cualquier otro.
- Realizar el acceso a los datos y su tratamiento, de conformidad con lo dispuesto en esta DPC, el Reglamento interno del PSC, y las instrucciones recibidas de la Comisión Directora.
- A no divulgar los datos de carácter personal a los que tuviera acceso durante la realización de sus funciones, así como a proteger el derecho al honor y a la intimidad de los afectados.
- A adoptar y cumplir las medidas técnicas y organizativas precisas para garantizar la seguridad de los *Sistemas, Ficheros, personas y procesos en los que se realice un acceso o tratamiento de Datos de Carácter Personal.* Dichas medidas quedarán reflejadas en el documento de seguridad definido en el Real Decreto de Medidas de Seguridad 1720/2007.
- A utilizar en su comunicación con el CORPME únicamente canales de comunicación seguros y protegidos mediante cifrado, así como los mecanismos de autenticación necesarios para el aseguramiento de la confidencialidad de las transmisiones.
- A restituir o eliminar, de conformidad con las instrucciones recibidas del responsable del Fichero, los datos personales de los que estuviese en posesión a la finalización de la relación con el CORPME, en caso de que por decisión de la Junta de Gobierno del CORPME, ejecutada por la Comisión Directora, de conformidad con el Reglamento del Servicio, alguna Unidad de Tramitación dejara de serlo.
- A recabar de Solicitantes y Suscriptores de certificados, en los procesos ante la Unidad de Tramitación, el consentimiento expreso para el tratamiento de sus datos personales, en cuanto resulte necesario para la prestación del Servicio de Certificación. Guardando constancia de dicho consentimiento a los efectos oportunos. En cualquier caso, y sin perjuicio de las autorizaciones expresas que oportunamente se soliciten del afectado en formularios y documentos del Servicio, se presumirá, en tanto que imprescindibles para la prestación del Servicio de Certificación solicitado, que el solicitante o el suscriptor otorga su consentimiento para el tratamiento de sus datos personales, únicamente en lo que se refiera a la prestación de dicho servicio.

La comunicación a terceros que confían en certificados digitales emitidos por el CORPME de los datos personales incorporados a dichos certificados, y que se publican en el Directorio de Certificados del CORPME. Se realizará de conformidad con lo dispuesto en el Artículo 11 de la LOPD. En tal sentido, el Suscriptor consiente, como presupuesto de la efectividad jurídica del servicio de certificación provisto por el CORPME, la publicación en el Directorio de Certificados de los datos personales asociados a la clave pública del certificado, la cual constituye para cualquier tercero el medio de verificación de la firma del suscriptor.

El acceso a la información contenida en la aplicación Agenda, que gestiona las citas para la emisión y renovación de certificados en las Unidades de Tramitación, y en las Listas de Revocación podrá realizarse por los terceros de buena fe, únicamente a los indicados efectos de verificación de la firma electrónica del suscriptor, prohibiéndose cualquier acceso a dichos datos y su recopilación para su posterior tratamiento y utilización para fines distintos a los descritos. Las infracciones consistentes en el volcado de datos, y su posterior tratamiento y uso para fines distintos a los autorizados, serán sancionables con multa de hasta 600.000 euros, y podrán dar lugar a las acciones penales y civiles procedentes.

En cualquier caso se garantiza a los Solicitantes y Suscriptores de Certificados Digitales del CORPME el libre ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición, previstos en la LOPD. El afectado deberá dirigir su solicitud al CORPME por escrito a la dirección postal del Servicio que figura en el apartado correspondiente de esta DPC.

9.4.3 Documento de Seguridad

9.4.3.1 Definición y alcance del Documento de Seguridad del CORPME

El CORPME y a los únicos efectos de la prestación del Servicio de Certificación, recaba durante el proceso de registro de usuario del solicitante en la agenda: (**https://www.registradores.org/scr/agenda**), o durante el proceso de emisión de certificados en la comparecencia personal del solicitante ante la Unidad de Tramitación, determinados datos personales de los Solicitantes y Suscriptores.

Como consecuencia del acceso y tratamiento que realiza de los referidos datos de carácter personal de los solicitantes y suscriptores, para la prestación del Servicio de Certificación el CORPME deberá adoptar las medidas de seguridad requeridas de conformidad con lo dispuesto en el Real Decreto 1720/2007, elaborando un documento de seguridad a tal efecto.

El documento de seguridad define y regula la aplicación de las medidas organizativas y de tipo técnico que garanticen la seguridad de los datos incorporados a los Ficheros de datos de los que el CORPME sea responsable. Disponiendo lo necesario para su conservación, salvaguarda de su integridad, confidencialidad y utilización legítima de acuerdo con el fin para el que fueron recabados.

Las medidas aplicables en virtud del Documento de Seguridad, se extenderán a las distintas áreas de actividad del CORPME como Autoridad de Certificación que emite Certificados Digitales Cualificados, así como a las Unidades de Tramitación que, de conformidad con el Reglamento 1720/2007 y la presente DPC, desarrollen funciones de Autoridad de Registro.

Todos los empleados del CORPME que tengan por razón de su actividad cualquier contacto directo o indirecto, habitual o incidental, con datos de carácter personal, o que participen de algún modo de su tratamiento, estarán vinculados por las políticas y controles definidos en el Documento de Seguridad. Se notificará por escrito a cada empleado el ámbito de sus responsabilidades en materia de protección de datos, así como los procedimientos y controles aplicables que le incumben en función de su puesto dentro de la organización. El empleado firmará a la recepción de la documentación de seguridad un documento que acredita su conocimiento y aceptación de las referidas obligaciones y responsabilidades que asume.

El documento de Seguridad del CORPME tiene el siguiente contenido:

- **Directrices Generales de Seguridad,** donde se enumeran las directrices generales de seguridad a implantar para las actividades relacionadas con la salvaguardia y seguridad de los Ficheros automatizados con Datos de Carácter Personal.
- **Organización de Seguridad**, donde se estructura y dimensiona la organización de seguridad que el CORPME establece para salvaguardar y asegurar la confidencialidad de todos los datos de carácter personal que maneja.
- **Sistemas de Información,** donde se identifican y describen los Sistemas de Información dependientes del CORPME a través de los cuales se realiza un tratamiento de Datos de Carácter Personal.
- **Normativa y Procedimientos**, donde se definen y describen un conjunto de Normas y Procedimientos necesarios y obligatorios para salvaguardar la información y asegurar la confidencialidad de los Datos de Carácter Personal de los Sistemas de Información del CORPME.

9.4.3.2 Roles en la ejecución de las políticas y protección de datos

El órgano responsable de la definición y ejecución de las políticas de seguridad es el Comité de Seguridad del CORPME el cual está constituido por:

- El Responsable Sistemas de Información del CORPME.
- Responsable de Seguridad LOPD del CORPME.
- Los Responsables de Explotación de las instalaciones del CORPME.

- Los Responsables departamentales de Ficheros con Datos de Carácter Personal (en adelante, DCP).

Así mismo tendrán participación en el Comité de Seguridad los Registradores integrantes de las comisiones de trabajo del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España, en las áreas de afinidad a la Protección de Datos.

Las funciones del Comité de Seguridad serán, entre otras, las siguientes:

- Estudio y análisis de las estrategias de seguridad.
- Designar al Responsable de Seguridad del CORPME para que coordine y controle la ejecución de las medidas de seguridad, normas y procedimientos definidos en este Documento de Seguridad. El Responsable de Seguridad, una vez nombrado, pasará a ser miembro del Comité de Seguridad.
- Análisis de las propuestas de modificación del Documento de Seguridad que elabore el Responsable de Seguridad.
- Análisis de las medidas correctoras a implantar, derivadas de los informes de auditoría que se realicen periódicamente en materia de seguridad de Datos de Carácter Personal.
- Revisión de los informes de verificación del correcto cumplimiento de lo dispuesto en el Documento de Seguridad LOPD, que emita el Responsable de Seguridad.
- Análisis de los informes explicativos de aquellas incidencias que afecten de manera grave a los Sistemas de Información, que emita el Responsable de Seguridad.
- Seguimiento de los diferentes Planes de Seguridad que se definan.
- Tratar cualquier otro tema que se considere de interés en materia de seguridad informática.

Sin perjuicio de la máxima responsabilidad en materia de protección de datos que ostenta el Comité de Seguridad, serán responsables de la implantación de las medidas objeto del documento de seguridad, en el ámbito de sus respectivas funciones, el Responsable del fichero y el Responsable de Seguridad.

9.4.3.2.1 Responsable del Fichero

El CORPME será Responsable de los Ficheros de datos personales a los que con ocasión del desempeño de sus funciones como Prestador de Servicios de Certificación, tenga acceso.

Las funciones que el Reglamento 1720/2007 pone a Cargo del Responsable del Fichero, serán desempeñadas por el responsable de cada departamento en el que se hayan de implantar medidas y controles de seguridad de conformidad con el documento de seguridad.

Las funciones del Responsable del Fichero son, entre otras, las que siguen:

- Elaborar e implantar el Documento de Seguridad de los Ficheros automatizados que contienen DCP's en el ámbito de su respectivo departamento.
- Adoptar las medidas necesarias para que el personal que accede a los Sistemas de Información con DCP's, conozca las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en que puede incurrir en caso de incumplimiento. Esta tarea la realiza en colaboración con el Responsable de Seguridad.
- Autorizar por escrito la ejecución de los procesos de recuperación de DCP's, según lo establecido en el Procedimiento de Recuperación de Datos de Carácter Personal.
- Establecer los criterios a seguir a la hora de conceder, alterar o anular el acceso autorizado de usuarios a los Sistemas de Información que manejan DCP's en el CORPME.
- Autorizar la salida de soportes informáticos que contengan Datos de Carácter Personal fuera de los locales donde se ubica el fichero, según los Procedimientos de Salida de Soportes Informáticos con Datos de Carácter Personal.
- Autorizar el uso de DCP's reales en las pruebas de las aplicaciones que manejan los ficheros con DCP's.

- Adoptar las medidas correctoras pertinentes para solventar las deficiencias que en materia de seguridad de DCP's se detecten tras la realización de las auditorias periódicas, tanto internas como independientes que habrán de realizarse.
- Autorizar los accesos, modificación y supresión de DCP's, solicitadas por los titulares de los datos según se describe en el Procedimiento de Ejecución de los Derechos de Acceso, Modificación y Supresión de DCP's.
- Si se diera el caso, incluir en los contratos de prestación de servicios que impliquen acceso a DCP's, las cláusulas que establezcan las obligaciones de la empresa que presta el servicio respecto a la seguridad de los DCP's que maneja.

9.4.3.2.2 Responsable de Seguridad

El Responsable de Seguridad coordina y controla todas las tareas y actividades que en materia de seguridad de DCP's se realicen en el CORPME. Asimismo se responsabiliza de la definición, implantación y supervisión de las Normas y Procedimientos que afectan a los Ficheros con DCP's.

Las funciones asignadas al Responsable de Seguridad del CORPME son las siguientes:

- Notificar para su inscripción en el Registro General de Protección de Datos, la creación, modificación y cancelación de los ficheros automatizados que contengan Datos de Carácter Personal.
- Mantener actualizado el Inventario de Ficheros con datos de carácter personal.
- Colaborar con el Responsable de Fichero en la definición de una colección de perfiles de usuario, donde se especifiquen las opciones de acceso permitido y el tipo de acceso requerido (actualización o consulta) a las aplicaciones que tratan los ficheros.
- Concretar los datos técnicos y administrativos para cumplimentar las peticiones de administración de usuarios derivadas de las necesidades manifestadas por los Responsables de las Áreas Usuarias.
- Autorizar las altas, bajas y modificaciones de acceso de los usuarios a los Sistemas de Información que manejan DCP's, siguiendo los criterios que para ello determine el Responsable de Fichero.
- Procesar la petición de usuarios mediante el mecanismo habilitado de actualización de identificados y contraseña de acceso.
- En la emisión de Datos de Carácter Personal desde el CORPME, solicitar al Responsable de Ficheros, la preceptiva autorización para la salida de soportes que contengan datos de carácter personal.
- Participar en los procesos de recuperación de DCP's, según lo establecido en el Procedimiento de Copias de Respaldo y Recuperación de Datos:
  - Verificar la definición y aplicación del Procedimiento de realización de Copias de Respaldo y Recuperación de Datos.
  - Comunicar al Responsable de Ficheros la necesidad de recuperación de datos para obtener la autorización a la misma.
  - Participar en la toma de decisiones asociadas a las recuperaciones de datos.
- Asesorar, en la definición de requisitos, sobre las medidas de seguridad que deben adoptarse en el desarrollo de aplicaciones que manejen DCP's. Validar que se han implantado los requisitos de seguridad necesarios.
- Mantenimiento actualizado del Documento de Seguridad LOPD:
  - Definir y establecer las Normas y Procedimientos que en materia de seguridad afecten a los Ficheros automatizados con DCP's.
  - Mantener actualizadas las Normas y Procedimientos que en materia de seguridad afecten a los ficheros automatizados con DCP's.
  - Mantener actualizada dentro del ámbito del Documento de Seguridad la información relativa a los Sistemas de Información que contienen DCP's.
  - Estar informado de los cambios que puedan producirse en las disposiciones legales sobre el tratamiento de Datos de Carácter Personal, y proponer medidas de adecuación a dichos cambios, y en particular a los cambios que alteren el Documento de Seguridad.
- Verificación del cumplimiento de lo dispuesto en el Documento de Seguridad LOPD:

  - Verificar periódicamente, según la Normativa para regular los controles periódicos para verificar lo dispuesto en el Reglamento 1720/2007, el correcto cumplimiento de las actuaciones que en materia de seguridad de DCP's se realicen en el CORPME.
  - Elaborar informes de verificación del cumplimiento de lo dispuesto en el Documento de Seguridad del CORPME y presentarlos, si lo estima conveniente, a la Comisión de Seguridad.
  - Creación, modificación y supresión de ficheros
  - Preparar las disposiciones de publicación en el BOE de la creación, modificación o supresión de ficheros del CORPME que contengan DCP's y sean de titularidad pública.
  - Comprobar periódicamente la coherencia de la información contenida en el Inventario de Ficheros con DCP's con la existente en el Documento de Seguridad LOPD.
- Colaboración en las Auditorías de Seguridad:
  - Controlar que la Auditoría de Seguridad LOPD se realice al menos cada dos años para los ficheros de nivel MEDIO Y ALTO, en caso de existir alguno.
  - Trasladar los informes de auditoría que periódicamente se realicen, al Responsable de Fichero.
  - Analizar los informes de Auditoría y si lo considera necesario, elevar las medidas correctoras a implantar a la Comisión de Seguridad para su aprobación.
  - Confirmar la existencia en el informe de auditoría, de una valoración sobre el nivel de adecuación de las medidas y controles al Reglamento 1720/2007, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias e incluyendo los hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
- Gestión de la Seguridad de los Sistemas de Información:
  - Supervisar y mantener actualizados los registros de usuarios con acceso autorizados a los sistemas de información.
  - Supervisar y analizar las incidencias de seguridad acaecidas en el CORPME en relación con la seguridad de los ficheros automatizados con DCP's.
  - Dictaminar medidas cuya aplicación minimice y/o elimine las incidencias acaecidas.
  - Revisar periódicamente la información de control registrada sobre los accesos de los usuarios a los Sistemas de Información (trazas de LOG) y elaborar periódicamente (al menos una vez al mes) un informe de las revisiones realizadas y los problemas detectados.
  - Reuniones de la Comisión de Seguridad:
    - Asistir y participar en las reuniones de la Comisión de Seguridad.
    - Presentar las propuestas que estime necesarias de modificación del Documento de Seguridad LOPD.
- Presentar los informes correspondientes a:
  - Auditorías de seguridad realizadas.
  - Verificación del cumplimiento de lo dispuesto en el Documento de Seguridad LOPD.
  - Incidencias de carácter grave ocurridas que afecten a la seguridad de los Datos de Carácter Personal.
  - Presentar cualquier otra propuesta de medidas y actuaciones relativas a la seguridad de los Datos de Carácter Personal.

9.4.3.3 Medidas y procedimientos de seguridad a implantar en ejecución del RD 1720/2007

A fin de cumplir con lo dispuesto en el título VIII se recogerán las siguientes medidas de seguridad de los datos personales tratados:

9.4.3.3.1 Medidas de control de acceso a las instalaciones del CORPME

Como se describió en el apartado correspondiente, el CORPME dispone de controles y medidas de seguridad para restringir el acceso de personas ajenas al servicio a las dependencias del CORPME. Además de las medidas preventivas, el CORPME llevará un registro de acceso a las salas de equipos de proceso de datos que sirvan de soporte a la actividad de prestador de servicios de certificación.

Dentro de las medidas de seguridad y control de accesos se definirá una política de control de llaves y Tarjetas de Identificación, correspondiendo la custodia de las llaves no expresamente asignadas, y la autorización para la copia y depósito de las mismas al Responsable de Seguridad. En la política se establecerán también los requisitos de seguridad aplicables en materia de identificación y custodia de llaves.

9.4.3.3.2 Medidas de control de acceso a la información: Política de Permisos

El CORPME elaborará un inventario de puestos con sus correspondientes niveles de autorización para el acceso y tratamiento de DCP's. Las autorizaciones de acceso se vincularán además de a usuarios concretos, a determinados equipos de proceso de datos, cuya ubicación y configuración por defecto estará orientada a asegurar la confidencialidad y protección de los DCP's.

La autorización de accesos a los datos contenidos en un fichero corresponde al Responsable del Fichero.

Los Responsables de Ficheros o las personas en quien estos deleguen, son los únicos con competencia para conceder, alterar o anular los accesos autorizados a los sistemas.

El Responsable de Seguridad, en colaboración con los Responsables de Fichero y Responsables Operativos, establecerá para cada sistema informático una segmentación de los accesos mediante la definición de perfiles de usuarios, donde se especifique las opciones de acceso permitidas y el tipo de acceso requerido (actualización o consulta).

Cada uno de los usuarios estará asignado a un perfil por cada sistema al que tenga acceso, de manera que exclusivamente tenga acceso autorizado a los recursos que precisa para desempeñar su función.

Cada usuario con acceso a los sistemas de la PKI, tendrá un llavero criptográfico con un certificado con las credenciales para acceder a los sistemas permitidos con los permisos correspondientes.

Cada acceso autorizado a los SS.II. deberá estar identificado unívocamente con el usuario correspondiente.

La generación de altas y bajas de usuario, así como la modificación de derechos de acceso de los usuarios, se tramitarán exclusivamente a través del medio establecido y siguiendo el procedimiento de administración de usuarios.

De cualquier modo, existirá un registro actualizado de los usuarios con acceso autorizado para cada sistema de información, al que tendrá acceso el Responsable de Seguridad en sus labores de verificación y control.

El registro de usuarios de cada sistema deberá contemplar al menos la siguiente información:

- Nombre de usuario.
- Cargo y puesto que desempeña en el CORPME.
- Perfil de usuario.

9.4.3.3.3 Accesos autorizados y Política de Contraseñas

- Todos los usuarios con acceso a un sistema de información, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- En los SS.II. se deberá habilitar un mecanismo que exija, como mínimo cada 60 días, el cambio de la contraseña para cada autorización de acceso.
- La longitud de las contraseñas será igual o superior a ocho (8) caracteres. El sistema de información, si lo permite, obligará al uso de esta longitud mínima de contraseña.
- Las contraseñas estarán constituidas por combinación de caracteres alfabéticos y numéricos y no hará referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.
- El sistema se inhabilitará para aquellos usuarios que intenten conectarse, de forma consecutiva, a través de identificadores y/o contraseñas incorrectas. El número máximo de intentos permitidos será de tres (3).
- Cuando un usuario tenga un periodo de inactividad en el acceso a un sistema de información mayor de setenta y cinco (75) días, siempre que tecnológicamente sea posible, se bloqueará la cuenta correspondiente.
- El sistema almacenará mediante algoritmos de cifrado las contraseñas, con el objeto de garantizar la confidencialidad e integridad de las mismas.

9.4.3.3.4 Registro de la información de acceso

Los SS.II. que manejen DCP's de nivel alto mantendrán automáticamente un fichero de registro (LOG) cuyo contenido se conservará al menos durante dos años y en el que se registrará como mínimo la siguiente información:

- Identificación de usuario que accede.
- Fecha y hora en que realizó el acceso.
- Fichero accedido.
- Tipo de acceso.
- Acceso autorizado o denegado.
- Clave u otra información que identifique los registros accedidos por el usuario.

Los mecanismos que permiten el registro de los datos son competencia directa del Responsable de Seguridad, sin que se deba permitir en ningún caso, la desactivación de los mismos.

9.4.3.3.5 Medidas de Seguridad para la gestión de soportes de almacenamiento físico de datos

El acceso a los soportes que contengan DCP's, deberá restringirse quedando únicamente a disposición de los usuarios autorizados. El almacenamiento deberá realizarse en locales adecuados en cuanto a las medidas de control ambiental y control de acceso físico. La conservación de los soportes deberá realizarse de manera sistemática, de conformidad con una política de identificación e inventariado llevada a cabo por uno o más empleados especializados que actuarán como responsables de la gestión de soportes.

9.4.3.3.6 Medidas de Seguridad aplicables a Sistemas Informáticos y redes de comunicaciones

El Responsable de Seguridad será el único autorizado para definir los procedimientos de asignación de permisos de uso y de accesos a los sistemas y redes de datos que permitan el acceso a los DCP's, de conformidad con los niveles de criticidad de los datos de que se trate, y de la propia estructura organizacional del CORPME.

El uso de sistemas y el acceso a través de una red de datos a los DCP's deberá estar condicionado a la posesión legítima e introducción correcta de los datos de acceso (nombre de usuario y contraseña) asignados al empleado del CORPME en razón a la función que desempeña y de acuerdo con la presente DPC.

Los intentos fallidos de acceso fraudulento, los cuales estarán en cualquier caso limitados a un número reducido de intentos a fin de evitar los ataques de fuerza bruta, serán objeto de registro a fin de poder ser investigados y perseguidos, guardándose la fecha, hora, código y claves erróneas que se han introducido, así cualquier otra información que permita identificar al responsable del acceso fallido.

9.4.3.3.7 Estructura de los Ficheros con datos de carácter personal

Los ficheros que contengan datos de carácter personal serán comunicados y registrados oportunamente en el Registro de Ficheros de la Agencia Española de Protección de Datos. La estructura de los mismos así como el nivel de los datos que contienen serán los definidos en la comunicación y registro inicial, correspondiendo la aprobación de cualquier modificación, y su comunicación a la Agencia Española de Protección de Datos al Responsable de Seguridad.

9.4.3.3.8 Gestión de Incidencias

Se habilitará un registro de incidencias del Servicio bajo la supervisión del Responsable de Seguridad, donde quedarán anotadas todas las incidencias surgidas con ocasión de la prestación del Servicio. En dicho Registro se anotará también la notificación de la incidencia al departamento que corresponda, para su indagación sobre la misma, registrándose así mismo el resultado de las gestiones practicadas para la resolución de la misma.

La falta de comunicación por parte del empleado que tuviera conocimiento de una incidencia en el servicio, al departamento correspondiente, constituirá una falta sancionable disciplinariamente.

El Registro de incidencias deberá incluir, al menos, la información siguiente: Fecha y hora de ocurrencia, descripción detallada de la misma, identidad de quien notifica la incidencia y de quien toma cuenta de ella; gravedad, estimada, de la incidencia; y respuesta ofrecida, una vez sea atendida.

Como método de detección y notificación de incidencias, el PSC del CORPME dispone de alarmas de seguridad para reportar actividades anormales en los sistemas.

El tiempo empleado para la notificación de cualquier incidente de seguridad de alto impacto a las partes interesadas está definido dentro un periodo de 24 horas desde su detección.

Las vulnerabilidades críticas se corrigen en un periodo de 48 horas después de su identificación.

9.4.3.3.9 Procedimientos de copias de seguridad y recuperación de datos

Además de garantizar la confidencialidad de los datos de carácter personal, es preciso también disponer las medidas y controles necesarios para asegurar la integridad y la disponibilidad de dichos datos para los fines a los que sirven. Congruentemente con lo expuesto se articularán procedimientos de copia de seguridad de tipo correctivo que permitan la recuperación de los datos en caso de eliminación accidental o maliciosa, corrupción de los ficheros o cualquier causa que haga imposible el acceso legítimo a los mismos.

La definición de los procedimientos operativos para la realización de copias de respaldo estará a cargo del Responsable de Seguridad. Así mismo será el Responsable de Seguridad el encargado, en caso de pérdida de ficheros, de gestionar la recuperación de los soportes con los datos de respaldo y su restauración en los repositorios en producción a partir de la información respaldada al momento inmediatamente anterior a la pérdida de los ficheros.

9.4.3.3.10 Política sobre Pruebas con datos reales

Con carácter general las pruebas de sistemas y aplicativos no se realizarán con datos reales. No obstante lo anterior cuando resulte imprescindible contar con dichos datos para la verificación del correcto funcionamiento de un sistema o aplicativo el Responsable de Seguridad, con autorización del Comité de Seguridad, dispondrá lo necesario para que dichas pruebas se realicen con las debidas garantías para la indemnidad e integridad de los datos.

9.5 Derechos de Propiedad Intelectual

De conformidad con la Ley de Propiedad Intelectual aprobada por RDL 1/1996, de 12 de abril, todos los derechos en materia de propiedad intelectual e industrial relacionados con los sistemas, documentos, procedimientos patentables, listas de revocación y cualesquiera otros, relacionados con su actividad como prestador de servicios de certificación, corresponderán en exclusiva al CORPME.

Los documentos y demás elementos del PSC del CORPME se referenciarán bajo la jerarquía del OID 17276 asignado por IANA al CORPME.

9.6 Representaciones y garantías

9.6.1 Obligaciones de las CA's

En particular, son obligaciones del Prestador de Servicios de Certificación las siguientes:

OCA.1. Realizar sus operaciones en conformidad con esta DPC y PC's de aplicación.

OCA.2. Proteger sus claves privadas.

OCA.3. Emitir certificados en conformidad con las PC's que les sean de aplicación.

OCA.4. Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 v3 y con los requerimientos de la solicitud.

OCA.5. Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.

OCA.6. No publicar los certificados de usuario salvo que así lo establezca la PC correspondiente.

OCA.7. Revocar los certificados en los términos descritos en la presente DPC y en las PC's y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web, con la frecuencia estipulada.

OCA.8. Publicar esta DPC y las PC's aplicables en el sitio Web referido en el presente documento.

OCA.9. Comunicar los cambios de esta DPC y de las PC's.

OCA.10. Conservar los documentos de Licencias de Uso de los certificados, en papel o electrónicamente, con los solicitantes de certificados en los que estos se dan por enterados de sus obligaciones y derechos, consienten en el tratamiento de sus datos personales por la CA y confirman que la información proporcionada es correcta.

OCA.11. Garantizar la disponibilidad de las CRL's.

OCA.12. En el caso que la CA proceda a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con lo estipulado en la presente DPC y PC's que les sea de aplicación.

OCA.13. Colaborar con las auditorías dirigidas por el PSC del CORPME para validar la renovación de las propias claves.

OCA.14. Operar de acuerdo con la legislación aplicable. En concreto con:

OCA.14.1. La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la Firma Electrónica.

OCA.14.2. La Ley 59/2003, de 20 de diciembre, de Firma Electrónica.

OCA.14.3. La L.O. 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.

OCA.15. Proteger, en caso de haberlas, las claves bajo su custodia.

OCA.16. No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados emitidos con el propósito de utilizarse para Firma Electrónica (key Usage = non repudiation).

OCA.17. En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ellas emitidos.

OCA.18. Conservar registrada toda la información y documentación relativa a los certificados durante quince (15) años contados desde su expedición.

9.6.2 Obligaciones de las RA's

En particular, son obligaciones de las Unidades de Tramitación:

ORA.1. Facilitar a los solicitantes los dispositivos informáticos adecuados para que puedan generar con las mayores garantías una pareja de claves asimétricas.

ORA.2. Comprobar la identidad del titular y las demás circunstancias de éste exigidas en las PC's, estableciendo en base a ellas el contenido del certificado.

ORA.3. Autorizar o denegar las solicitudes de emisión y revocación de certificados.

ORA.4. Notificar inmediatamente a la Unidad Técnica la revocación de cualquier certificado.

ORA.5. Formalizar las licencias de uso de los certificados con el titular, archivándolas junto a la documentación que se indique en las PC's, durante un período de quince (15) años a contar desde la fecha de caducidad o revocación del certificado.

ORA.6. Certificar, cuando le sea solicitado por el CORPME u otra persona con interés legítimo, que el solicitante ha sido convenientemente identificado y que la información sobre él aparecida en el certificado se corresponde con los datos obrantes en la Unidad.

ORA.7. Aplicar los controles de seguridad física y lógica, de procedimiento y personales, establecidos en el Plan de Seguridad.

ORA.8. Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del certificado y en el proceso de suspensión/revocación del mismo.

Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC.

9.6.3 Obligaciones de los titulares de los certificados

En particular, son obligaciones del Suscriptor las siguientes:

OS.1. Suministrar a las Unidades de Tramitación información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.

OS.2. Informar a los responsables de PKI de CORPME de cualquier modificación de esta información.

OS.3. Conocer, aceptar y firmar la licencia de uso del certificado.

OS.4. Usar el certificado para los fines para los que fue emitido, de acuerdo con las PC's aplicables.

OS.5. Custodiar diligentemente el dispositivo de creación de firma y la contraseña que protege el acceso a la clave privada de Firma Electrónica.

OS.6. Informar al CORPME a la mayor brevedad posible, y por cualquiera de los canales habilitados al efecto, la existencia de alguna causa de revocación del certificado.

OS.7. Abstenerse de utilizar la clave privada del certificado desde el mismo momento en el que se solicita o es advertido por la CA o la RA de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.

OS.8. Destruir el certificado cuando así lo exija la CA, en virtud del derecho de propiedad que en todo caso conserva sobre el Certificado y cuando el Certificado caduque o sea revocado.

OS.9. No monitorizar, manipular o realizar actos de "ingeniería inversa" sobre la implantación técnica (hardware y software) de los servicios de certificación, sin permiso previo por escrito de la CA.

OS.10. No transferir ni delegar sus responsabilidades sobre un certificado que le haya sido asignado a un tercero.

OS.11. Instalar el certificado únicamente en servidores que sean accesibles a los subjectAltName(s) enumerados en el perfil del certificado.

OS.12. Responder a las instrucciones de la CA en relación con el compromiso de la clave o el uso indebido del certificado dentro de un periodo de tiempo especificado.

OS.13. Reconocer y aceptar que la CA tiene derecho a revocar inmediatamente si el solicitante viola las condiciones de uso o si descubre que el certificado está siendo usado en actividades criminales, como fraude o distribución de malware.

Cualquier otra que se derive de la ley, de esta DPC o de las PC's.

9.6.4 Obligaciones de los terceros que confían o acepten los certificados

En particular, son obligaciones del Tercero las siguientes:

OTC.1. Verificar, antes de depositar su confianza en un certificado, que el mismo está vigente y no ha sido revocado. A tal fin deberá comprobar la validez y vigencia del certificado de firma por alguno de los medios disponibles: consulta de las listas de revocación (CRL's) o Consulta en línea de estado de certificados mediante protocolo OCSP, antes de aceptar cualquier comunicación o documento firmado digitalmente con uno de los certificados emitidos por el CORPME.

OTC.2. Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la PC correspondiente.

OTC.3. Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.

OTC.4. Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía.

OTC.5. Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.

Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

9.6.5 Obligaciones de la TSA

En particular, son obligaciones de la TSA las siguientes:

OTSA.1. Operar de acuerdo a esta DPC y a las políticas y procedimientos internos que sean de aplicación.

OTSA.2. Llevar a cabo revisiones internas y externas para asegurar el cumplimiento de la legislación de aplicación y las políticas y procedimientos internos.

OTSA.3. Proporcionar acceso ininterrumpido a los servicios de sellado de tiempo excepto en caso de interrupciones programadas, pérdidas de la sincronización temporal o causas de fuerza mayor.

9.6.6 Obligaciones de la VA

En particular, son obligaciones de la VA las siguientes:

OVA.1. Operar de acuerdo a esta DPC y a las políticas y procedimientos internos que sean de aplicación.

OVA.2. Llevar a cabo revisiones internas y externas para asegurar el cumplimiento de la legislación de aplicación y las políticas y procedimientos internos.

OVA.3. Proporcionar acceso ininterrumpido a los servicios de validación de certificados on-line, excepto en caso de interrupciones programadas, pérdidas de la sincronización temporal o causas de fuerza mayor.

9.6.7 Obligaciones de otros participantes

En particular, son obligaciones de otros participantes las siguientes:

El Servicio de Repositorio ha de mantener accesible para los Titulares y Terceros Aceptantes la información de los certificados que han sido revocados, en formato CRL.

9.7 Exención de responsabilidades

El CORPME responderá por el uso de los certificados que emite en los términos previstos en la presente DPC, las políticas aplicables a cada clase de certificado, así como en la Ley 59/2003 de Firma Electrónica, en la Ley 24/2001, y en las Instrucciones dictadas en materia de Firma Electrónica registral por la Dirección General de los Registros y el Notariado y demás normas que la desarrollen.

La responsabilidad del CORPME no se extenderá a las vulnerabilidades inherentes a los algoritmos criptográficos utilizados en el sistema de firma, definidos como estándares de referencia por los organismos competentes. No obstante lo anterior, el CORPME velará diligentemente porque sus sistemas se adecuen en cada momento al estado de la técnica.

El CORPME no será responsable por los daños sufridos por el suscriptor o un tercero, como consecuencia del uso de sus certificados, fuera de los supuestos de utilización expresamente admitidos. No podrá tampoco exigirse ninguna responsabilidad por daños al CORPME, siempre que éste pueda probar que su actividad como Prestador de Servicios de Certificación se ha desarrollado de plena conformidad con la Ley 59/2003 y demás leyes aplicables, la presente DPC y las PC's asociadas a cada clase de certificado.

El CORPME no responderá, en ningún caso, de la utilización que los suscriptores hagan de los certificados, ni de los errores de hecho o de interpretación que puedan cometer quienes validen una firma.

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.

El CORPME no será responsable en ningún caso cuando se den las siguientes circunstancias:

- Cuando concurran circunstancias consideradas de fuerza mayor, como catástrofes naturales, Guerras, y demás calamidades que provoquen una interrupción prologada de los servicios y suministros necesarios para la prestación del servicio.
- Los daños y perjuicios, directos o indirectos, causados por la utilización de los certificados y de las claves certificadas para usos no permitidos o fuera de su período de vigencia, así como por la pérdida o divulgación de la clave privada del suscriptor.

- Cuando el uso de los certificados se realice fuera de los casos permitidos, o se trate de certificados revocados o suspendidos y el interesado no verifique el estado del mismo antes de otorgarle su confianza.
- Compromiso de la clave privada, por revelación voluntaria del suscriptor o intervención maliciosa de un tercero, y pérdida o sustracción del soporte con los datos de creación de firma.
- Por el uso indebido, erróneo o fraudulento de los certificados o de las listas de Certificados Revocados (CRL), emitidas por el CORPME.
- Por la pérdida irrevocable de información debida al uso de un certificado digital del CORPME para el Cifrado de Confidencialidad.
- En caso de aportación de documentación falsificada o fraudulenta por parte del solicitante del certificado.
- Daños ocasionados por el mal uso de la información contenida en el certificado.
- La CA no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se autentiquen mediante un certificado emitido por ella.
- Los fallos o errores debidos a los equipos informáticos, navegadores o aplicaciones utilizados por el titular o por los terceros usuarios de los certificados.
- Los daños o perjuicios directos o indirectos que sean consecuencia de los procedimientos o productos empleados para generar la pareja de claves asimétricas a certificar cuando sea el propio solicitante quien aporte las claves.
- El contenido de los documentos firmados con una firma digital basada en un certificado emitido por él, ni por la información contenida en un servidor por el certificado

El CORPME responderá por los daños irrogados al Suscriptor o al tercero de buena fe que deposite su confianza en los certificados del CORPME, cuando medie dolo o culpa del prestador. El régimen de responsabilidad aplicable será el definido en la Ley 59/2003, de Firma Electrónica y en el resto de la legislación aplicable.

Sin perjuicio de lo indicado anteriormente se delimita el ámbito de responsabilidad asumido por el CORPME a los extremos siguientes:

- Garantizar la exacta correspondencia entre la información contenida en los certificados y la facilitada por el suscriptor en el momento de la emisión.
- Entregar al suscriptor un certificado de la misma clase del solicitado.
- Poner a disposición del suscritor en el DSCF correspondiente, la clave privada correspondiente a la pública identificada en el certificado entregado, garantizando la plena complementariedad de ambas claves.
- Mantener las listas de certificados revocados y el servicio de validación OCSP, permanentemente actualizados y accesibles.

Demás supuestos previstos en la legislación vigente según los cuales el Prestador de Servicios de Certificación haya de responder por los daños causados.

9.8 Limitaciones de las Responsabilidades

9.8.1 Responsabilidad de las RA's

Las Unidades de Tramitación autorizados por el CORPME son responsables de comprobar que los datos del certificado solicitado son correctos de acuerdo a la documentación presentada por el solicitante, siendo en todo caso responsable el prestador de servicios de certificación, de conformidad con el artículo 13.5 de la Ley de Firma Electrónica. Esta comprobación, se refiere tanto a los datos personales como a los cargos públicos o pertenencia a colectivo profesional, mediante el certificado o documento oficial correspondiente. De igual manera, las Unidades de Tramitación serán responsables del archivado de toda documentación relacionada con los certificados y sus solicitudes, debiendo archivarse por un mínimo de quince (15) años.

Las Unidades de Tramitación no son responsables cuando el incumplimiento se deba a un caso fortuito o fuerza mayor o si queda fuera de su control, tales como desastres naturales o de otro tipo, cortes en el suministro eléctrico o funcionamiento defectuoso de los sistemas de comunicaciones, siempre que se disponga de las medidas de seguridad estándar. Tampoco son responsables cuando los daños se deban al incumplimiento, por parte de los suscriptores o terceros, de alguna de sus obligaciones, en particular por la no verificación de las CRL's actualizadas o si el suscriptor del certificado excede el límite del mismo en cuanto a su posible uso o al importe del valor de las transacciones que pueden realizarse con los mismos.

9.8.2 Responsabilidad de la TSA

La TSA no asumirá responsabilidad alguna en relación al uso de los sellos de tiempo emitidos para cualquier actividad no especificada en la presente DPC y en las PC's.

La TSA no se responsabiliza del contenido de los datos a los que se aplique el sello de tiempo que emita y no responde de posibles daños y perjuicios en transacciones a las que se haya aplicado.

La TSA no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

9.8.3 Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente DPC, el PSC del CORPME no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

9.9 Indemnizaciones

9.9.1 Indemnizaciones por daños ocasionados por PKI del CORPME

El CORPME asumirá las indemnizaciones correspondientes por daños efectuados a terceros en base a los términos establecidos en la ley 59/2003, de 20 de diciembre, de Firma Electrónica, su reglamentación y la presente DPC. Ninguna otra responsabilidad será asumida por el PSC del CORPME ante titulares de certificados o terceros que confíen o acepten los certificados.

9.9.2 Indemnizaciones por los daños causados por los Suscriptores

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado electrónico durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones según lo establecido en la ley 59/2003, de 20 de diciembre, de Firma Electrónica.

9.9.3 Indemnizaciones por los daños ocasionados por los Terceros que confían

Tanto suscriptores como terceros son responsables por apoderarse, destruir, modificar, adulterar, indebidamente los datos de una firma o certificado electrónico durante o después de la fecha de creación del certificado y son sujetos a indemnizaciones según lo establecido en la ley 59/2003, de 20 de diciembre, de Firma Electrónica.

9.10 Período de validez

9.10.1 Plazo

Esta DPC entrará en vigor desde el momento de su publicación en el directorio web del CORPME y estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión.

9.10.2 Sustitución y derogación de la DPC

Esta DPC 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 DPC quede derogada se retirará del directorio web del CORPME, si bien se conservará durante quince (15) años.

9.10.3 Efectos de la finalización

Las obligaciones y restricciones que establece esta DPC, 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

Las vías de comunicación ante cualquier notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC son:

- Correo electrónico (Producirá sus efectos una vez el destinatario al que van dirigidas haya recibido la comunicación).
- Correo certificado (Dirigido a la dirección contenida en el apartado 1.10 del presente documento).
- Teléfono de contacto recogido en el apartado 1.10 del presente documento.

9.12 Procedimientos de cambios en las especificaciones

9.12.1 Procedimiento para los cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre la DPC y las PC's del PSC del CORPME es la Autoridad de Aprobación de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado 1.7 del presente documento.

9.12.2 Circunstancias en las que el OID debe ser cambiado

Si los cambios de las especificaciones, a juicio de la AAP, no afectan a la aceptabilidad de los certificados, se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados correspondientes a la PC o DPC modificada.

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. Por último, también se modificarán los dos últimos números del Identificador de Objeto (OID) que lo representa. Para este tipo de modificaciones se comunicará a los usuarios de los certificados correspondientes a la PC o DPC modificada.

9.13 Reclamaciones

Todas las reclamaciones entre usuarios y el CORPME deberán ser comunicadas por la parte en disputa al CORPME, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir con relación a esta DPC o a las PC's publicadas, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales españoles, con independencia del lugar dónde se hubieran utilizado los certificados emitidos.

9.14 Normativa Aplicable

Las operaciones y funcionamiento del PSC del CORPME, así como la presente DPC y las PC's que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la Firma Electrónica.
- Reglamento UE 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 59/2003, de 20 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

9.14.1 Cumplimiento de la Normativa Aplicable

La Autoridad de Aprobación de Políticas tiene la responsabilidad de velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

9.15 Estipulaciones diversas

9.15.1 Cláusula de aceptación completa

Todos los Terceros que Confían asumen en su totalidad el contenido de la última versión de esta DPC y de las PC's que sean de aplicación.

9.15.2 Independencia

En el caso de que cualquiera de los apartados recogidos en la presente DPC sea declarado, parcial o totalmente, nula o ilegal no afectará tal circunstancia al resto del documento.

9.15.3 Resolución por la vía judicial

Todas las reclamaciones entre usuarios y CORPME deberán ser comunicadas por la parte en disputa a CORPME, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir con relación a esta DPC o a las PC's, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales españoles, con independencia del lugar dónde se hubieran utilizado los certificados emitidos.

9.16 Otras estipulaciones

No estipulado.

10 ANEXOS

10.1 Declaración de Prácticas de Certificación del CORPME

El presente documento constituye un resumen de los derechos y obligaciones contenidos en la **Declaración de Prácticas de Certificación** del **Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España**. El presente extracto tiene carácter no-exhaustivo y no exonera al usuario final de la obligación de consultar la Declaración completa para informarse adecuadamente de sus obligaciones como titular de un certificado digital y de sus derechos ante el CORPME.

La DPC y las políticas particulares de Certificación aplicables a cada tipo de certificado, regulan todos los aspectos relativos al ciclo de vida de los certificados, en particular aquellos referidos la solicitud, emisión, aceptación, renovación, reemisión y revocación de los mismos.

Las relaciones jurídicas entre el emisor de los certificados, los usuarios de los mismos y los terceros que confían en los certificados del CORPME, se desarrollarán dentro del marco definido por la DPC y las políticas particulares que resulten de aplicación a cada clase de certificado.

El CORPME emite distintos tipos de certificados, tanto a personas físicas (en su condición de particulares como en el ejercicio de una profesión, cargo o representación) como personas jurídicas en los casos en los que corresponda. Será responsabilidad del solicitante de un certificado del CORPME consultar las condiciones de uso aplicables, proveer la documentación justificativa de los atributos a certificar. La utilización del certificado de Firma Electrónica para fines no recogidos en sus PC's, se hará bajo la entera responsabilidad del suscriptor.

Será responsabilidad del Suscriptor ejercer una custodia diligente del DSCF y de la contraseña que protege el acceso a su clave privada. En caso de compromiso de dicha clave, o cualquier otro supuesto, pérdida o sustracción del dispositivo, que entrañe un riesgo de uso ilegítimo de la Firma Electrónica del suscriptor, éste deberá notificar de manera inmediata al CORPME para proceder a la Revocación del certificado.

Cualquier variación en los datos proporcionados al CORPME en el momento de solicitar el certificado, o la modificación o cese en el cargo o representación certificada, deberá ser comunicada de inmediato al CORPME a fin de revocar el certificado y, en su caso, emitir uno nuevo que recoja fielmente las nuevas circunstancias del suscriptor.

La Declaración de Prácticas de Certificación en su última versión, así como el resto de documentos vinculados con la prestación del servicio serán accesibles en la URL **http://pki.registradores.org/normativa/index.htm**.

Para cualquier consulta relacionada con el servicio puede dirigirse a la dirección contenida en la siguiente URL: **http://pki.registradores.org/normativa/direccion.html.**