Servicio de Certificación Digital

Organización Médica Colegial de España

Declaración de Prácticas de Certificación
Entidad de Certificación de la
Organización Médica Colegial

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación documento	ASTREA	10/12/2006
1.1	Sección 5	Separación de los controles por dominios	ASTREA	31/06/2009
	En todo el documento	Actualización al Real Decreto 1720/2007, de 21 de diciembre, nuevo reglamento de desarrollo de la Ley de Protección de Datos		
2.0	En todo el documento	Inclusión de dos nuevos certificados: • Médico externo • Persona jurídica en software	ASTREA	24/09/2011
2.1	En todo el documento	Cambios tras la inspección del Ministerio de Industria	ASTREA	02/07/2012
2.2	En todo el documento	• Ampliación de los subscriptores del certificado de persona jurídica. • Ampliación de los certificados en tarjeta para separar funciones de identificación, firma y cifrado. • Se añade el certificado en software para personal administrativo	ASTREA	21/05/2013
3	En todo el documento	• Cambio del proveedor técnico de certificados. • Cambios en los procesos de emisión de las tarjetas. • Se añade el certificado en HSM. • Se elimina el certificado de órgano colegial. • La Orden HAP/800/2014 se incluye como referencia en los certificados de software.	ASTREA	16/01/2015

Tabla de contenido

1 Introducción

La política de certificación de la Organización Médica Colegial establece un sistema de certificación con los siguientes objetivos:

1) La regulación de la emisión y gestión de la tarjeta de médico colegiado, con la condición de dispositivo seguro de creación de firma electrónica.
2) La emisión y gestión, por uno o más prestadores de servicios de certificación, de certificados reconocidos de firma electrónica de médico colegiado y otro personal colegial, así como de otros servicios de certificación, que se prestarán sobre la tarjeta de médico.
3) La acreditación, por la Organización Médica Colegial, de los diferentes prestadores de servicios de certificación que suministren certificados a los profesionales colegiados, al objeto de garantizar la calidad y seguridad en la emisión y gestión de los citados certificados.
4) La prestación de servicios de validación y re-certificación a entidades, públicas y privadas, sobre los certificados, al objeto de garantizar la actualidad y validez de las informaciones corporativas, incluidas o no en los certificados, y en especial, de la condición de médico.

En concreto, la política de certificación ha definido los requisitos comunes tanto para la expedición de certificados por la Entidad de Certificación de la Organización Médica Colegial, o por cualquier otro prestador de servicios de certificación corporativos, que debe ser acreditado por la Organización Médica Colegial, como para la validación y, en su caso, re-certificación de la condición corporativa de médico y otras informaciones, para certificados expedidos por cualesquiera prestadores de servicios de certificación, en las diferentes aplicaciones en que resulte necesario.

Todo ello se realiza sobre la base de la tarjeta médica colegial como instrumento de identificación y firma del médico colegiado, así como, en su caso, de otro personal colegial, frente a otros profesionales colegiales, las entidades y corporaciones públicas y privadas, y las Administraciones Públicas.

1.1 Presentación

Este documento declara las prácticas de certificación de firma electrónica de la Entidad de Certificación de la Organización Médica Colegial.

Los certificados que se emiten son los siguientes:

- Certificados **corporativos** de:
  - Médico/a colegiado/a en tarjeta
  - Médico/a colegiado/a en software
  - Médico/a colegiado/a en HSM (Hardware centralizado)
  - Personal administrativo en tarjeta.
  - Personal administraivo en software
  - Colegio/Entidad/Persona jurídica en tarjeta.
  - Colegio/Entidad/Persona jurídica en software.
- Certificados **externos** de:
  - Médico empleado público en tarjeta.

Los servicios de certificación prestados por la Entidad de Certificación de la OMC se encuentran integrados en la jerarquía de la Autoridad de Certificación de Camerfirma, y por este motivo resultan reconocidos internacionalmente y son interoperables con las principales aplicaciones, como el correo electrónico seguro o las aplicaciones de firma de documentos basadas en el sistema operativo Microsoft Windows.

AC Camerfirma, S.A. fue creada en el año 1999, con el objetivo de dotar de seguridad a las comunicaciones y operaciones telemáticas realizadas en el ámbito empresarial.

La integración de la Entidad de Certificación de la OMC dentro de la jerarquía de la Autoridad de Certificación de Camerfirma se ha realizado mediante la firma del certificado de la Entidad de Certificación de la OMC, de acuerdo con lo establecido en la Política de Certificación de la Global Chambersign Root v1.0, de 23 de julio de 2003, a la que se sujeta la presente Declaración.

1.2 Nombre del documento e identificación

Este documento es la “Declaración de Prácticas de Certificación de la Organización Médica Colegial”.

1.2.1 Identificadores de certificados actuales

La Organización Médica Colegial ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Tipo de certificado	**OID**
Certificados corporativos	.1
Certificado de colegiado en tarjeta:	https://www.cgcom.es/CertCol
• para identificación	1.3.6.1.4.1.26852.1.1.1.1
• para firma	1.3.6.1.4.1.26852.1.1.1.2
• para cifrado	1.3.6.1.4.1.26852.1.1.1.3
Certificado de personal administrativo en tarjeta:	https://www.cgcom.es/CertAdmin
• para identificación	1.3.6.1.4.1.26852.1.1.2.1
• para firma	1.3.6.1.4.1.26852.1.1.2.2
• para cifrado	1.3.6.1.4.1.26852.1.1.2.3
Certificado de persona jurídica en tarjeta:	https://www.cgcom.es/CertJur
• para identificación	1.3.6.1.4.1.26852.1.1.3.1
• para firma	1.3.6.1.4.1.26852.1.1.3.2
• para cifrado	1.3.6.1.4.1.26852.1.1.3.3
Certificados de persona jurídica en software:	https://www.cgcom.es/CertJurSoft
• para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.5
Certificado de personal administrativo en software:	https://www.cgcom.es/CertAdminSoft
• para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.6
Certificados de médico colegiado en software	https://www.cgcom.es/CertColSoft

• para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.7
Certificados de médico colegiado en HSM	https://www.cgcom.es/CertColHSM
• para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.9
Certificados externos	.2
Certificados de médico empleado público en tarjeta	https://www.cgcom.es/CertMEP
• para identificación	1.3.6.1.4.1.26852.1.2.1.1
• para firma	1.3.6.1.4.1.26852.1.2.1.2
• para cifrado	1.3.6.1.4.1.26852.1.2.1.3

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas de Certificación.

1.2.2 Identificadores de certificados obsoletos

Tipo de certificado	**OID**	**Funciones**
Certificados corporativos obsoletos	.1	
Certificados de colegiado en tarjeta	1.3.6.1.4.1.26852.1.1.1	Identificación, firma y cifrado
Certificados de personal administrativo en tarjeta	1.3.6.1.4.1.26852.1.1.2	Identificación, firma y cifrado
Certificados de persona jurídica en tarjeta	1.3.6.1.4.1.26852.1.1.3	Identificación, firma y cifrado
Certificado de órgano colegial en tarjeta	1.3.6.1.4.1.26852.1.1.4	Identificación, firma y cifrado
Certificado de órgano colegial en tarjeta (I)	1.3.6.1.4.1.26852.1.1.4.1	Identificación
Certificado de órgano colegial en tarjeta (F)	1.3.6.1.4.1.26852.1.1.4.2	Firma
Certificado de órgano colegial en tarjeta (C)	1.3.6.1.4.1.26852.1.1.4.3	Cifrado
Certificado de órgano colegial en software	1.3.6.1.4.1.26852.1.1.8	Identificación, firma y cifrado

Certificados externos obsoletos	.2	
Certificados de médico empleado público en tarjeta	1.3.6.1.4.1.26852.1.2.1	Identificación, firma y cifrado

1.3 Participantes en los servicios de certificación

Los servicios descritos en esta declaración de prácticas son prestados a una comunidad profesional de usuarios, que obtienen certificados para diversos usos y aplicaciones profesionales relacionadas con las entidades que integran la Organización Médica Colegial, y aquellas otras entidades del ámbito sanitario con las que la OMC disponga un convenio de colaboración.

La OMC no expide los certificados corporativos al público, ni siquiera cuando se trata de certificados reconocidos, como el certificado de firma de colegiado.

1.3.1 Prestador de Servicios de Certificación

Los prestadores de servicios de certificación son personas, físicas o jurídicas, que expiden y gestionan certificados para entidades finales, que se denominan suscriptores o titulares de certificados.

El papel de la Organización Médica Colegial es doble:

- Por una parte, la OMC garantiza la calidad en el empleo de los medios electrónicos, informáticos y telemáticos por los profesionales médicos, mediante la acreditación de los prestadores de servicios de certificación, de acuerdo con la política de certificación.
- Por otra parte, la OMC dispone de una Entidad de Certificación para la emisión y gestión de claves y certificados de entidad final, incluyendo personas, dentro del ámbito corporativo, a los propios colegios y otras personas jurídicas del ámbito sanitario, y a médicos empleados públicos de Servicios Autonómicos de Salud.

1.3.2 Registradores

En general, los registradores de certificados corporativos son las entidades de la Organización Médica Colegial, y en especial, los Colegios de Médicos.
La Organización Medica Colegial asiste técnicamente en el registro a los Colegios de Médicos.

1.3.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para firma, autenticación y cifrado.

Serán entidades finales del sistema de certificación de la Organización Médica Colegial las siguientes entidades:

1) Solicitantes de certificados.
2) Suscriptores de certificados.
3) Poseedores de claves.
4) Terceros que confían en certificados.

1.3.3.1 Solicitantes de certificados

Todo certificado debe ser solicitado por una persona, en su propio nombre o en nombre de una organización.

Pueden ser solicitantes:

1) El colegio que va a ser el futuro suscriptor del certificado. Dicho colegio puede establecer un modelo de solicitud de certificado por parte de los colegiados.
2) Una persona autorizada por dicho futuro suscriptor.
3) El Servicio Autonómico de Salud, que puede establecer un modelo de solicitud de certificado por parte de sus médicos-empleados públicos.
4) Otras personas jurídicas del ámbito sanitario que dispongan de convenio con la OMC.

1.3.3.2 Suscriptores de certificados

Los suscriptores son los colegios, otras personas jurídicas del ámbito sanitario y los Servicios Autonómicos de Salud identificados en los certificados

El suscriptor tiene licencia de uso del certificado, y otorga el certificado a un poseedor de claves, debidamente autorizado, y que figura identificado en el certificado, como se indica a continuación.

1.3.3.3 Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves de firma digital y de descifrado, pudiendo ser colegiados/as, personal administrativo , custodios de certificados de persona jurídica y médicos empleados públicos de Servicios Autonómicos de Salud.

Los poseedores de claves se encuentran debidamente autorizados para ello por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de descifrado no puede ser recuperada, actualmente, por el prestador de servicios de certificación, por lo que los poseedores de claves son los únicos responsables de su protección y deberían considerar las implicaciones de perder una clave privada de descifrado, dado que puede implicar la pérdida de documentos cifrados. No obstante, la EC-OMC está desarrollando un procedimiento para custodiar de forma confidencial y segura la clave privada de descifrado.

1.3.3.4 Terceros que confían en certificados

Los terceros que confían en certificados son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, los terceros deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes condiciones generales de la contratación.

1.3.4 Otros participantes

1.3.4.1 Proveedores técnicos

La Entidad de Certificación de la OMC se apoya en los servicios de certificación que ofrece el proveedor técnico CAMERFIRMA,

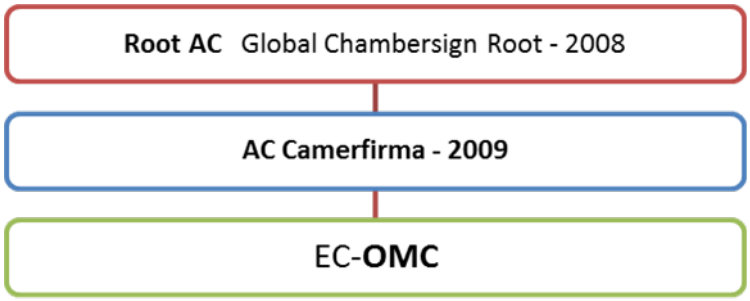
Asimismo, la EC-OMC se apoya en los servicios de mantenimiento y soporte sobre el producto smartCMS que ofrece el proveedor técnico BIT4ID IBERICA.

1.3.4.2 Jerarquías externas de certificación

Como se ha indicado anteriormente, los certificados se integran en la jerarquía de Camerfirma, lo que garantiza su reconocimiento e interoperabilidad.

1.3.5 Jerarquía de Certificación

La jerarquía de Certificación en la que se integra la Entidad de Certificación de la OMC es la siguiente



1.3.5.1 Root AC – Autoridad de Certificación Raíz

Es la certificación raíz de la jerarquía que emite certificados a otras Autoridades de Certificación, y cuyo certificado de clave pública ha sido autofirmado.

Los datos de identificación del Certificado Raíz actual de AC Camerfirma SA son:

- CN: *Global Chambersign Root - 2008*
- SHA1 hash: *4ABD EEEC 950D 359C 89AE C752 A12C 5B29 F6D6 AA0C*
- Válido desde: *Viernes, 01 de agosto de 2008*
- Válido hasta: *Sábado, 31 de Julio de 2038*
- Longitud de clave RSA: *4096 bits*

Esta Jerarquía (Global Chambersign Root (JCS) 1.3.6.1.4.1.17326.10.1.1) está creada por AC Camerfirma SA para la emisión de certificados bajo proyectos concretos a nivel internacional, con una/s determinada/s Entidad/es entre las que se encuentra la EC-OMC.

1.3.5.2 AC Camerfirma – Autoridad intermedia

Es la entidad de certificación dentro de la jerarquía que emite los Certificados Intermedios de Nivel 2 y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz.
Los datos de identificación del actual Certificado Intermedio de Nivel 1, generado y gestionado por AC Camerfirma SA se detallan a continuación:

- CN: *AC Camerfirma - 2009*
- SHA1 hash: *BABA 69CF D5CC C94D 056B 5BE7 805F E203 CBEB 5C57*
- Válido desde: *Lunes, 16 de marzo de 2009*
- Válido hasta: *Domingo, 11 de marzo de 2029*
- Longitud de clave RSA: *4096 bits*

El OID de AC Camerfirma – 2009 es: 1.3.6.1.4.1.17326.10.4.1.

1.3.5.3 EC-OMC – Autoridad de certificación de nivel 2

Es la entidad de certificación dentro de la jerarquía que emite los certificados de entidad de los usuarios finales, y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Intermedia de Nivel 1 mencionada anteriormente.
Este certificado Intermedio de Nivel 2 también ha sido generado por AC Camerfirma SA, pero es gestionado por la EC-OMC como Entidad de Certificación acreditada para emitir los certificados finales a suscriptores.
En este caso, AC Camerfirma SA actuará como prestador de servicios de certificación para la la Entidad de Certificación de la Organización Médica Colegial (EC-OMC).
La EC-OMC tiene la siguiente Autoridad de Certificación Intermedia de Nivel 2, cuya información más relevante es:

- CN: *OMC*
- SHA1 hash: *E764 1564 BEA7 35BE F73A 4ECF 2D3E 070B B75E 3F2B*
- Válido desde: *Lunes, 24 de Noviembre de 2014*
- Válido hasta: *Jueves, 21 de Noviembre de 2024*
- Longitud de clave RSA: *2048 bits*

El OID de la EC-OMC en la jerarquía de certificación es “anypolicy”: 2.5.29.32.0

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1 Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, visibles en el web https://certificacion.cgcom.es

1.4.1.1 Certificado corporativo de colegiado/a en tarjeta

Los certificados corporativos de colegiado son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los certificados corporativos de colegiado funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados se emiten a colegiados del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso. Este colegiado tiene la consideración de poseedor de claves y de la tarjeta y el software complementario correspondientes.

Asimismo garantizan la condición de colegiado, dada la intervención obligatoria del colegio en el procedimiento de emisión del certificado, actuando como entidad de registro o como garante de la información.

1.4.1.1.1 Certificado corporativo de colegiado/a para identificación

Este certificado con OID 1.3.6.1.4.1.26852.1.1.1.1 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados corporativos de colegiado (de identificación) garantizan la identidad del subscriptor y del poseedor de la clave privada de identificación.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas las siguientes funciones:
    a. Digital Signature (para realizar la función de autenticación)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación” del médico colegiado/a”.

1.4.1.1.2 Certificado corporativo de colegiado/a para firma

Este certificado con OID 1.3.6.1.4.1.26852.1.1.1.2 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados corporativos de colegiado (de firma) permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Por otra parte, los certificados corporativos de colegiado (de firma) se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas las siguientes funciones:
    a. Content commintment (para la realización de la función de firma electrónica)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida de médico colegiado/a”.

1.4.1.1.3 Certificado de cifrado para colegiado, en tarjeta

Este certificado con OID 1.3.6.1.4.1.26852.1.1.1.3 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados de cifrado se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

a) La clave pública del poseedor de claves indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Key Encipherment
b. Data Encipherment

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   c. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.

c) El campo “User Notice” nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.2 Certificado corporativo de personal administrativo en tarjeta

Los certificados corporativos de personal administrativo son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los certificados corporativos de personal administrativo funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados se emiten a personal administrativo del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso. Este órgano tiene la consideración de poseedor de claves y de la tarjeta y el software complementario correspondientes.

1.4.1.2.1 Certificado corporativo de personal administrativo para identificación

Este certificado con OID 1.3.6.1.4.1.26852.1.1.2.1 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados corporativos de personal administrativo (de identificación) garantizan la identidad del subscriptor y del poseedor de la clave privada de identificación.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Digital Signature (para realizar la función de autenticación)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación de personal administrativo y de servicios”.

1.4.1.2.2 Certificado corporativo de personal administrativo para firma

Este certificado con OID 1.3.6.1.4.1.26852.1.1.2.2 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados corporativos de personal administrativo (de firma) permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Asimismo, incluyen una manifestación relativa a la categoría del poseedor de claves, que han sido comprobados antes de emitir el certificado, y son correctos. Es necesario advertir que esta indicación no es, por si sola, suficiente por determinar las facultades que tiene el poseedor de claves para firmar en nombre del subscriptor; por lo tanto, el usuario del certificado tendrá que comprobar las facultades y poderes de firma del poseedor mediante otros medios, diferentes al certificado, como por ejemplo el servicio de validación de la OMC.

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita, puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Content commintment (para la realización de la función de firma electrónica)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida de personal administrativo y de servicios”.

1.4.1.2.3 Certificado de cifrado de personal administrativo, en tarjeta

Este certificado con OID 1.3.6.1.4.1.26852.1.1.2.3 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados de cifrado se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

c) La clave pública del poseedor de claves indicada en el certificado.
d) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Key Encipherment
    b. Data Encipherment
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.

c) El campo “User Notice” nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.3 Certificado corporativo de persona jurídica en tarjeta

Los certificados corporativos de persona jurídica en tarjeta son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los certificados corporativos de persona jurídica en tarjeta funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de persona jurídica en tarjeta son certificados para el colegio y otras entidades del ámbito sanitario, a emplear en aplicaciones de Administraciones Públicas que expresamente admitan certificados de persona jurídica, y no son emitidos al público en ningún caso. La persona que recibe el certificado de persona jurídica en tarjeta tiene la consideración de poseedor y responsable de custodia de las claves, así como de la tarjeta y el software complementario correspondientes.

1.4.1.3.1 Certificado corporativo de persona jurídica para identificación

Este certificado con OID 1.3.6.1.4.1.26852.1.1.3.1 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados corporativos de persona jurídica (de identificación) en tarjeta garantizan la identidad del subscriptor y del poseedor de la clave privada de identificación.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Digital Signature (para realizar la función de autenticación)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.

c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación de la persona jurídica”.

1.4.1.3.2 Certificado corporativo de persona jurídica para firma

Este certificado con OID 1.3.6.1.4.1.26852.1.1.3.2 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados corporativos de persona jurídica (de firma) permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Por otra parte, los certificados corporativos de persona jurídica (de firma) se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del subscriptor, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

La firma electrónica generada usando estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, cuando menos, esta firma habrá sido producida con el dispositivo seguro.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
   a. Content commintment (para la realización de la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida de persona jurídica”.

1.4.1.3.3 Certificado de cifrado para persona jurídica, en tarjeta

Este certificado con OID 1.3.6.1.4.1.26852.1.1.3.3 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados de cifrado se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

e) La clave pública del poseedor de claves indicada en el certificado.
f) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Key Encipherment
    b. Data Encipherment
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.4 Certificado corporativo de persona jurídica en software

Este certificado dispone del OID 1.3.6.1.4.1.26852.1.1.5.

Los certificados corporativos de persona jurídica en software de firma electrónica avanzada son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de persona jurídica en software no funcionan necesariamente con dispositivos seguros de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados corporativos de persona jurídica en software son certificados para el colegio y otras entidades del ámbito sanitario, a emplear en aplicaciones de Administraciones Públicas que expresamente admitan certificados de persona jurídica, y no son emitidos al público en ningún caso. La persona que recibe el certificado de persona jurídica tiene la consideración de poseedor y responsable de custodia de las claves, así como del software complementario correspondiente.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la “Orden HAP/800/2014, de 9 de mayo, por la que se establecen normas específicas sobre sistemas de identificación y autenticación por medios electrónicos con la Agencia Estatal de Administración Tributaria”), que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

Por otra parte, los certificados corporativos de persona jurídica en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital.

Finalmente, los certificados corporativos de persona jurídica en software se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

a) La clave pública del poseedor de claves indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que la OMC no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
    c. Cifrado de claves
    d. Cifrado de datos
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida y cifrado de persona jurídica en software”.

1.4.1.5 Certificado corporativo de personal administrativo en software

Este certificado dispone del OID 1.3.6.1.4.1.26852.1.1.6.

Los certificados corporativos de personal administrativo en software de firma electrónica avanzada son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de personal administrativo en software no funcionan necesariamente con dispositivos seguros de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Estos certificados se emiten a personal administrativo del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la “Orden HAP/800/2014, de 9 de mayo, por la que se establecen normas específicas sobre sistemas de identificación y autenticación por medios electrónicos con la Agencia Estatal de Administración Tributaria”), que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

Por otra parte, los certificados corporativos de personal administrativo en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

d) Autenticación en sistemas de control de acceso.
e) Firma de correo electrónico seguro.
f) Otras aplicaciones de firma digital.

Finalmente, los certificados corporativos de personal administrativo en software se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

c) La clave pública del poseedor de claves indicada en el certificado.
d) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que la OMC no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

d) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
    c. Cifrado de claves
    d. Cifrado de datos
e) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
f) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida y cifrado del personal administrativo en software”.

1.4.1.6 Certificado corporativo de colegiado en software

Este certificado dispone del OID 1.3.6.1.4.1.26852.1.1.7.

Los certificados corporativos de colegiado en software de firma electrónica avanzada son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de colegiado en software no funcionan necesariamente con dispositivos seguros de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Estos certificados se emiten a colegiados del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la “Orden HAP/800/2014, de 9 de mayo, por la que se establecen normas específicas sobre sistemas de identificación y autenticación por medios electrónicos con la Agencia Estatal de Administración Tributaria”), que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

Por otra parte, los certificados corporativos de colegiado en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

g) Autenticación en sistemas de control de acceso.
h) Firma de correo electrónico seguro.
i) Otras aplicaciones de firma digital.

Finalmente, los certificados corporativos de colegiado en software se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

e) La clave pública del poseedor de claves indicada en el certificado.
f) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que la OMC no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

g) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
    c. Cifrado de claves
    d. Cifrado de datos
h) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
i) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida y cifrado del médico colegiado, en software”.

1.4.1.7 Certificado corporativo de colegiado en HSM

Este certificado dispone del OID 1.3.6.1.4.1.26852.1.1.9.

Los certificados corporativos de colegiado en HSM (hardware centralizado) de firma electrónica reconocida son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de colegiado en HSM funcionan necesariamente con dispositivos seguros de creación de firma electrónica, centralizados en un HSM (Hardware Security Module), de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Estos certificados se emiten a médicos colegiados del ámbito corporativo del colegio suscriptor y no son emitidos al público en ningún caso.

Por otra parte, los certificados corporativos de colegiado en HSM se pueden utilizar en otras aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital.

Finalmente, los certificados corporativos de de colegiado en HSM se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

g) La clave pública del poseedor de claves indicada en el certificado.
h) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que la OMC no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

j) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
   a. Firma digital
   b. No repudio
   c. Cifrado de claves
   d. Cifrado de datos

k) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.

l) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida y cifrado del de colegiado en HSM”.

1.4.1.8 Certificado externo de médico empleado público en tarjeta

Los certificados externos de médico empleado público son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estos certificados permiten identificar a los médicos como personas al servicio de la Administración Pública, vinculándolos con ésta, siguiendo los requisitos establecidos en la Ley 11/2007, de 23 de junio, de aceso electrónico de los ciudadanos a los servicios públicos.

Los certificados externos de médico empleado público funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados externos de médico empleado se emiten de acuerdo con el Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009

Los certificados se emiten a médicos empleados públicos del ámbito del Servicio Autonómico de Salud suscriptor, y no son emitidos al público en ningún caso. El médico

empleado público tiene la consideración de poseedor de claves y, de la tarjeta y el software complementario correspondientes.

Asimismo garantizan la condición de médico, dada la intervención obligatoria del colegio en el procedimiento de emisión del certificado, actuando como entidad de registro o como garante de la información.

1.4.1.8.1 Certificado externo de médico empleado público (identificación)

Este certificado con OID 1.3.6.1.4.1.26852.1.2.1.1 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados externos de médico empleado público (de identificación) garantizan la identidad del subscriptor y del poseedor de la clave privada de identificación

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Digital Signature (para realizar la función de autenticación)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación de médico del servicio autonómico de salud”.

1.4.1.8.2 Certificado externo de médico empleado público (firma)

Este certificado con OID 1.3.6.1.4.1.26852.1.2.1.2 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados externos de médico empleado público (de firma) permiten la generación de la “firma electrónica reconocida”; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se

equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Por otra parte, los certificados externos de médico empleado público (de firma) se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del subscriptor, como las aplicaciones que se indican a continuación:
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma digital.

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Content commintment (para la realización de la función de firma electrónica)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica reconocida de médico del servicio autonómico de salud”.

1.4.1.8.3 Certificado de cifrado para médico externo, en tarjeta

Este certificado con OID 1.3.6.1.4.1.26852.1.2.1.3 es emitido por la Entidad de Certificación de la OMC a partir del año 2013.

Los certificados de cifrado se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

a) La clave pública del poseedor de claves indicada en el certificado.

b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Key Encipherment
    b. Data Encipherment
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como reconocido.
c) El campo “User Notice” nos describe que el uso de este certificado es para la función de cifrado.

1.4.2 Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web http://certificacion.cgcom.es

El empleo de los certificados digitales en operaciones que contravienen la Política de Certificación, esta DPC, los documentos jurídicos vinculantes con cada certificado o los Contratos o Convenios con las entidades de Registro o con sus Firmantes/Suscriptores tiene la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la Autoridad de Certificación, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

La Autoridad de Certificación no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la EC OMC emitir valoración alguna sobre dicho contenido, asumiendo por tanto el signatario cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado. Asimismo, le será imputable al signatario cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en la Política de Certificación, esta DPC, los documentos jurídicos vinculantes con cada certificado o los Contratos o Convenios con las entidades de Registro o con sus Firmantes/Suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.4.2.1 Certificados corporativos en software

La información de límites en el perfil de certificado nos indica lo siguiente:

a) La ausencia de la indicación “QcSSCD (0.4.0.1862.1.4)” en el campo “Qualified Certificate Statements” indica el uso del certificado exclusivamente en software.

1.4.2.2 *Certificados en tarjeta*

La información de límites en el perfil de certificado nos indica lo siguiente:

a) La existencia de la indicación "QcSSCD (0.4.0.1862.1.4)" en el campo "Qualified Certificate Statements" limita el certificado a su uso de forma obligatoria con un dispositivo seguro de creación de firma.

1.5 Administración de la política

1.5.1 Organización que administra el documento

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA –
ORGANIZACIÓN MÉDICA COLEGIAL
PLAZA DE LAS CORTES, 11- 28014 MADRID
TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

1.5.2 Datos de contacto de la organización

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA –
ORGANIZACIÓN MÉDICA COLEGIAL
PLAZA DE LAS CORTES, 11- 28014 MADRID
TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de la Entidad de Certificación de la OMC garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

2 Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

La Entidad de Certificación de la OMC dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.
Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la Entidad de Certificación de la OMC, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación.

2.2 Publicación de información del prestador de servicios de certificación

La Entidad de Certificación de la OMC publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento del poseedor de claves
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.
- Las condiciones generales de la contratación aplicables a los suscriptores y a los terceros que confían en certificados.

2.3 Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.
La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de esta Declaración de Prácticas de Certificación.

2.4 Control de acceso

La Entidad de Certificación de la OMC no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

La Entidad de Certificación emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si el poseedor de claves ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Identificación y autenticación

3.1 Registro inicial

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y del poseedor de claves, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1 Certificado corporativo de colegiado/a

Country (C)	"ES"
Organization (O)	Colegio profesional
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertCol (c)06"
Surname	Apellidos
Given Name	Nombre
Title	"Médico colegiado/a"
Serial Number	DNI/NIE
Common Name (CN)	Nombre, apellidos y número de colegiado/a

3.1.1.2 Certificado corporativo de personal administrativo

Country (C)	"ES"
Organization (O)	Colegio profesional
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertAdmin (c)06"
Surname	Apellidos

Given Name	Nombre
Title	"Personal administrativo y de servicios"
Serial Number	DNI/NIE
Common Name (CN)	Nombre y apellidos

3.1.1.3 Certificado corporativo de persona jurídica en tarjeta

Country (C)	"ES"
Organization (O)	Colegio profesional o entidad jurídica del ámbito sanitario
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertJur (c)06"
Surname	Apellidos del custodio
Given Name	Nombre del custodio
1.3.6.1.4.1.18838.1.1	DNI/NIE
Serial Number	NIF de la entidad
Common Name (CN)	Colegio profesional u otra persona jurídica del ámbito sanitario

3.1.1.4 Certificado externo de médico empleado público

Country (C)	"ES"
Organization (O)	Servicio Autonómico de Salud
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertECSAS (c)09"
Surname	Apellidos + " – " + NIF del empleado
Given Name	Nombre
Title	"Certificado electrónico de empleado público médico"
Serial Number	DNI/NIE del empleado público
Common Name (CN)	Nombre, apellidos + " – " + NIF del empleado
DNI/NIE del responsable - OID 2.16.724.1.3.5.3.2.4	DNI/NIE del responsable

Número de identificación de personal - OID 2.16.724.1.3.5.3.2.5	Número de identificación del médico como empleado público
Nombre de pila - OID 2.16.724.1.3.5.3.2.6	Nombre de pila del médico – empleado público.
Primer apellido - OID 2.16.724.1.3.5.3.2.7	Primer apellido del médico – empleado público
Segundo apellido - OID 2.16.724.1.3.5.3.2.8	Segundo apellido del médico – empleado público

3.1.1.5 Certificado corporativo de persona jurídica en software

Country (C)	"ES"
Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertJurSoft (c)11"
Surname	Apellidos del custodio
Given Name	Nombre del custodio
1.3.6.1.4.1.18838.1.1	DNI/NIE
Serial Number	NIF de la entidad
Common Name (CN)	Colegio profesional u otra persona jurídica del ámbito sanitario

3.1.1.6 Certificado corporativo de colegiado/a en software

Country (C)	"ES"
Organization (O)	Colegio profesional
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertColSoft"
Surname	Apellidos
Given Name	Nombre
Title	"Médico colegiado/a"

Serial Number	DNI/NIE
Common Name (CN)	Nombre, apellidos y número de colegiado/a

3.1.1.7 Certificado corporativo de colegiado/a en HSM

Country (C)	"ES"
Organization (O)	Colegio profesional
Organizational Unit (OU)	"Condiciones de uso en https://www.cgcom.es/CertColHSM"
Surname	Apellidos
Given Name	Nombre
Title	"Médico colegiado/a"
Serial Number	DNI/NIE
Common Name (CN)	Nombre, apellidos y número de colegiado/a

3.1.2 Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural y serán interpretados de acuerdo con la legislación española aplicable a los nombres de las personas físicas y jurídicas.

3.1.3 Empleo de anónimos y seudónimos

En general no se pueden utilizar seudónimos para identificar una organización.

Se pueden utilizar seudónimos en certificados personales siempre que en caso necesario se pueda determinar su identidad.

En ningún caso se emiten certificados de anónimos.

3.1.4 Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley española, en sus propios términos.

El campo “país” siempre será España, dado que el certificado muestra la relación entre un colegiado, un empleado o un órgano y un colegio profesional español, o un empleado público y un Servicio Autonómico de Salud español, con independencia de la nacionalidad del colegiado, empleado u órgano. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, empleado u órgano la persona autorizada a su uso, o bíen es suscriptor el Servicio Autonómico de Salud, y un médico empleado público suyo la persona autorizada a su uso.
El campo “número de serie” debe incluir el DNI o el NIE del colegiado, empleado, órgano o médico empleado público al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.
En el caso de los certificados de persona jurídica, de acuerdo con la normativa tributaria, el campo "número de serie" debe incluir el NIF de la persona jurídica, mientras que el campo identificado con el número "1.3.6.1.4.1.18838.1.1", debe incluir el DNI o el NIE del custodio.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de la Entidad de Certificación de la OMC.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Documento Nacional de Identidad, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) de la persona física
- Código de Identificación Fiscal (CIF) de la empresa
- Tipo de Certificado (Campo descripción del certificado).
- Dispositivo (Ubicación del certificado: Movil, HSM, Tableta…)

3.1.6 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

La Entidad de Certificación de la OMC no estará obligada a determinar previamente que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación española, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

3.2 Validación inicial de la identidad

La identidad de los suscriptores de certificados corporativos, son las entidades que integran la Organización Médica Colegial u otras entidades jurídicas del ámbito sanitario, resulta fijada de antemano, y la identidad de los poseedores de claves de dichos certificados corporativos – colegiados/as, órganos colegiales y personal administrativo – se valida mediante los registros corporativos de la entidad.

La identidad de los suscriptores de certificados externos, que como se ha dicho son los Servicios Autonómicos de Salud, resulta fijada de antemano, y la identidad de los poseedores de claves de dichos certificados externos como empleados públicos se valida mediante los registros del Servicio Autonómico de Salud, así como la identidad como médicos se valida mediante los registros del CGCOM.

La identidad de los suscriptores en otras entidades jurídicas del ámbito sanitario resulta fijada de antemano. Será necesario disponer para los servicios de certificación digital de un convenio entre la OMC y estas entidades. La identificación de los trabajadores de estas entidades se validan mediante sus registros internos y la identidad como médicos se valida mediante los registros del CGCOM.

A estos efectos, la Organización Médica Colegial dispone de un sistema de registro que garantiza la corrección y consistencia de las informaciones contenidas en dichos registros corporativos.

Los ficheros personales del sistema de registro se encuentran inscritos en la Agencia Española de Protección de Datos, por la Organización Médica Colegial.

3.2.1 Prueba de posesión de clave privada

El par de claves es generado por la Entidad de Certificación de la OMC, en su caso asistido por las entidades indicadas en la sección 1.3.4.1 de esta Declaración de Prácticas de Certificación, por delegación del solicitante, durante el proceso de personalización final del dispositivo seguro de creación de firma del suscriptor.

En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado y, cuando corresponda, del correspondiente dispositivo seguro y par de claves almacenados en su interior.

3.2.2 Autenticación de la identidad de una organización

3.2.2.1 Colegios de Médicos, CGCOM y OMC

No se requiere realizar procedimiento de autenticación de la existencia de la organización titular del certificado en certificados corporativos, dado que la organización forma parte del ámbito corporativo de la Organización Médica Colegial y por tanto se encuentra fijada de antemano.

La identidad de los Colegio Oficiales de Médicos

La Ley 2/1974, de 13 de febrero, de Colegios Profesionales, indica en su artículo 1.1 que "*los Colegios Profesionales son Corporaciones de derecho publico, amparadas por la Ley y reconocidas por el Estado, con personalidad jurídica propia y plena capacidad para el*

cumplimiento de sus fines". Asimismo, su artículo 1.3, en redacción dada por Ley 25/2009, de 22 de diciembre, establece que "*son fines esenciales de estas Corporaciones la ordenación del ejercicio de las profesiones, la representación institucional exclusiva de las mismas cuando estén sujetas a colegiación obligatoria, la defensa de los intereses profesionales de los colegiados y la protección de los intereses de los consumidores y usuarios de los servicios de sus colegiados, todo ello sin perjuicio de la competencia de la Administración Pública por razón de la relación funcionarial*".
La Ley 2/1974 establece en su artículo 4.1 que "*la creación de Colegios Profesionales se hará mediante Ley, a petición de los profesionales interesados*" y, en su apartado 4, que "*cuando estén constituidos varios Colegios de la misma profesión de ámbito inferior al nacional existirá un Consejo General cuya naturaleza y funciones se precisan en el artículo noveno*".

La identidad del Consejo General de Colegios de Médicos y de la Organización Médica Colegial

El artículo 9.1 de la Ley 2/1974 indica que "*Los Consejos Generales de los Colegios tienen a todos los efectos la condición de Corporación de Derecho público, con personalidad jurídica propia y plena capacidad. Tendrán las siguientes funciones*:

> *[…]*
> *b) Elaborar los Estatutos generales de los Colegios, así como los suyos propios.*
> *c) aprobar los Estatutos y visar los Reglamentos de régimen interior de los Colegios.*
> *d) Dirimir los conflictos que puedan suscitarse entre los distintos Colegios.*
> *e) Resolver los recursos que se interpongan contra los actos de los Colegios.*
> *f) Adoptar las medidas necesarias para que los Colegios cumplan las resoluciones del propio Consejo Superior dictadas en materia de su competencia.*
> *g) Ejercer las funciones disciplinarias con respecto a los miembros de las Juntas de Gobierno de los Colegios y del propio Consejo."*

La disposición adicional tercera de la Ley 2/1974, indica que "1. Se entiende por organización colegial el conjunto de corporaciones colegiales de una determinada profesión. 2. Son corporaciones colegiales el Consejo General o Superior de Colegios, los Colegios de ámbito estatal, los Consejos Autonómicos de Colegios y los Colegios Profesionales".

Los Estatutos de la Organización Médica Colegial de España, aprobados por Real Decreto 1018/1980, de 19 mayo, por el que se aprueban los Estatutos generales de la Organización Médica Colegial y del Consejo General de Colegios Oficiales de Médicos, en lo relativo a los

Estatutos generales del Consejo General de Colegios Oficiales de Médicos, indican en su artículo 1 que "*la Organización Médica Colegial se integra por los Colegios Provinciales Oficiales de Médicos y por el Consejo General*", y que "*la representación legal del Consejo General y de los Colegios, tanto en juicio como fuera de él, recaerá en los respectivos Presidentes* […]", en sentido análogo al artículo 7.4 de la Ley 2/1974. Finalmente, que "*corresponde a la Organización Médica Colegial la representación exclusiva de la profesión médica, la ordenación en el ámbito de sus competencias de la actividad profesional de los colegiados y la defensa de sus intereses profesionales*."

Los Estatutos del Consejo General de Colegios Oficiales de Médicos de España, aprobados por Real Decreto 757/2006, de 16 de junio, indica en su artículo 1 que "*El Consejo General de Colegios Oficiales de Médicos, es el órgano que agrupa, coordina y representa a todos los Colegios Oficiales de Médicos a nivel estatal y tiene, a todos los efectos, la condición de Corporación de Derecho Público con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines*."

El artículo 4 del RD 757/2006 establece que "*La Asamblea General es el máximo órgano rector del Consejo General y estará integrada por todos los Presidentes de los Colegios Oficiales de Médicos, por los miembros de la Comisión Permanente, por los Representantes Nacionales de las Secciones Colegiales que de conformidad con las disposiciones estatutarias estén constituidas y por los representantes de la Universidad, de las Sociedades Científicas y de otras entidades médicas que, con voz pero sin voto, la propia Asamblea acuerde incorporar*."

3.2.2.2 Servicio Autonómico de Salud

No se requiere realizar procedimiento de autenticación de la existencia del Servicio Autonómico de Salud titular del certificado en certificados externos, dado que se encuentra fijada de antemano.

La existencia de los Servicios Autonómicos de Salud le consta al Consejo General de Colegios Oficiales de Médicos por su relación institucional permanente con las Administraciones públicas, con el Ministerio y las Consejerías correspondientes.

La prestación del servicio se formaliza mediante el oportuno convenio de colaboración con el Servicio Autonómico de Salud.

3.2.2.3 Sociedades profesionales

La identificación para la expedición de certificados de persona jurídica a Sociedades profesionales queda garantizada por el registro correspondiente en cada Colegio de Médicos. La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, en su artículo 5.2 establece que "*para garantizar de forma efectiva y facilitar el ejercicio de los derechos a que se refiere el apartado anterior, los colegios profesionales, consejos autonómicos y consejos generales, en sus respectivos ámbitos territoriales, establecerán los registros públicos de profesionales que, de acuerdo con los requerimientos de esta ley, serán accesibles a la población y estarán a disposición de las Administraciones sanitarias*".

3.2.2.4 Fundaciones

No se requiere realizar procedimiento de autenticación de la existencia de cada una de las fundaciones titulares del certificado en certificados corporativos, dado que dichas fundaciones forman parte del ámbito corporativo de la Organización Médica Colegial y por tanto se encuentra fijada de antemano.

La identidad de las Fundaciones de la Organización Médica Colegial
La Ley 50/2002, de 26 de diciembre, de Fundaciones, indica en su artículo 2 que "Son fundaciones las organizaciones constituidas sin fin de lucro que, por voluntad de sus creadores, tienen afectado de modo duradero su patrimonio a la realización de fines de interés general. Las fundaciones se rigen por la voluntad del fundador, por sus Estatutos y, en todo caso, por la Ley."

Asimismo, el artículo 4 de dicho texto legal establece, en relación a la personalidad jurídica de las mismas, que dispondrán de ella desde la inscripción de la escritura pública de su constitución en el correspondiente Registro de Fundaciones. La inscripción sólo podrá ser denegada cuando dicha escritura no se ajuste a las prescripciones de la Ley.

La Organización Médica Colegial dispone de 3 fundaciones en el seno de su ámbito corporativo, lo cual se observa de los estatutos que las regulan:

- ***Fundación patronato de huérfanos y protección social de médicos "Príncipe de Asturias***", cuyos estatutos disponen:

  "Artículo 1º. Denominación y naturaleza. Bajo la denominación de "FUNDACIÓN PATRONATO DE HUÉRFANOS Y PROTECCIÓN SOCIAL DE MÉDICOS "PRINCIPE DE ASTURIAS" se constituye una Fundación de interés general y carácter particular, organización privada sin ánimo de lucro bajo el patrocinio del Consejo General de Colegios Médicos de España, que estará tutelada por el Protectorado que actualmente desempeña el Ministerio de Trabajo y Asuntos Sociales.

  Artículo 2º. Personalidad y capacidad. La Fundación está inscrita en el Registro de Fundaciones, tiene personalidad jurídica propia y plena capacidad de obrar, a tenor de lo dispuesto en el artículo 35 del Código Civil, pudiendo en consecuencia realizar todos aquellos actos que sean necesarios para el cumplimiento de los fines para los que ha sido creada, con sujeción a lo establecido en el Ordenamiento Jurídico."

- ***Fundación red de colegios médicos solidarios***, cuyos estatutos disponen:

  "Artículo 2.- Personalidad y capacidad. La Fundación constituida, una vez inscrita en el Registro de Fundaciones, tiene personalidad jurídica propia y plena capacidad para obrar, pudiendo realizar, en consecuencia, todos aquellos actos que sean necesarios para el cumplimiento de la finalidad para la que ha sido creada, con sujeción a lo establecido en el ordenamiento jurídico."

  "Art. 11.- Naturaleza del Patronato y de la Junta Rectora.
  El órgano de gobierno, representación y administración de la Fundación es el Patronato, por tanto, la Junta Rectora actuará dentro de las limitaciones legales y siempre por delegación de facultades del mismo. Su mandato será el equivalente al del cargo que desempeñen como miembros de la Asamblea General del Consejo General de Colegios Oficiales de Médicos. Finalizado su mandato se convocarán elecciones para cubrir los cargos de patronos que quedaron vacantes."

- ***Fundación para la formación de la Organización Médica Colegial***, cuyos estatutos disponen:

Artículo 21 . - El Patronato es el órgano supremo de gobierno, administración y representación de la Fundación: Serán miembros natos del Patronato los siguientes:

- Presidente. Que será el que obtenga igual cargo en el Consejo Oficial de Médicos.
- Vicepresidente. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.
- Secretario. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.
- Vicesecretario. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.
- Tesorero. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.
- Serán igualmente miembros de Patronato 5 Vocales designados por elección de entre y por los miembros que integran la Asamblea General de la O.M.C.

3.2.2.5 Otras entidades jurídicas del ámbito sanitario

No se requiere realizar procedimiento de autenticación de la existencia de otras entidades jurídicas del ámbito sanitario, dado que se encuentra fijada de antemano.

Se define a estas entidades jurídicas del ámbito sanitario como a aquellas entidades donde se ofrecen un conjunto de servicios que se proporcionan al individuo, con el fin de promover, proteger y restaurar su salud, donde tienen cabida la prevención, el tratamiento y el manejo de la enfermedad y la preservación del bienestar mental y físico a través de los servicios ofrecidos por los profesionales médicos y afines.

La existencia de estas entidades jurídicas del ámbito sanitario (como Hospitales, Clínicas, Centros de Salud, etc.) le consta al Consejo General de Colegios Oficiales de Médicos por su relación institucional permanente y por la relación laboral de muchos de sus miembros – los médicos colegiados en los Colegios Oficiales de Médicos- con dichas entidades jurídicas del ámbito sanitario.

La prestación del servicio de certificación digital se formaliza mediante el oportuno convenio de colaboración entre la Entidad de Certificación de la OMC y cada una de estas entidades jurídicas del ámbito sanitario.

3.2.2.6 *Para todos los casos*

Se comprueban, la autorización del solicitante de certificados y la existencia del dominio de correo electrónico corporativo.

3.2.3 Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1 *En certificados corporativos*

Los registros colegiales, que se integran en el Sistema de Registro son los únicos que legalmente permiten acreditar la condición de médico colegiado/a.
Los datos de los órganos colegiales y del personal administrativo se encuentran en otros registros colegiales.
Por este motivo, la información de identificación de poseedores de claves de certificados corporativos se valida comparando la información de la solicitud con los registros del Colegio correspondiente, asegurando la corrección de la información a certificar.

3.2.3.2 *En certificados externos*

Los registros colegiales que se integran en el Sistema de Registro son los únicos que legalmente permiten acreditar la condición de médico.
Los registros de personal de los Servicios Autonómicos de Salud son los únicos que legalmente permiten acreditar la condición de empleado público.
Por este motivo, la información de identificación de poseedores de claves de certificados externos se valida comparando la información de la solicitud con los registros colegiales y personales indicados, asegurando la corrección de la información a certificar.

3.2.3.3 *Necesidad de presencia personal*

En general, no se requiere presencia física directa para la obtención de certificados, ya que dicha presencia se ha producido anteriormente y los registros se mantienen permanentemente actualizados.

Sin embargo, antes de la emisión y entrega de un certificado de firma electrónica, la Entidad de Certificación de la OMC deberá contrastar la identidad del poseedor de claves de certificados mediante la presencia física directa o indirecta del mismo.

Durante este trámite, que puede diferirse al momento de entrega y aceptación del certificado y, en su caso, del dispositivo seguro de creación de firma y que se ejecuta con la colaboración del Colegio, de la Entidad jurídica del ámbito sanitario o del Servicio Autonómico de Salud solicitante, se confirma fehacientemente la validación de la identidad de la persona.

3.2.3.4 Vinculación de la persona física con una organización

La justificación documental de la vinculación del poseedor de la clave con el Colegio, la Entidad jurídica del ámbito sanitario o del Servicio Autonómico de Salud es la propia solicitud y su presencia en el registro de médicos del Colegio (para colegiados), en otros registros internos (para personal administrativo u órganos colegiados) o bien de empleados del Servicio Autonómico.

3.2.4 Información de suscriptor no verificada

La Entidad de Certificación de la OMC no incluye ninguna información de suscriptor no verificada en los certificados.

3.3 Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, la Entidad de Certificación de la OMC comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de renovación por parte del suscriptor.
- El uso de una "frase de comprobación de identidad", que consiste en información que sólo conoce el poseedor de claves, y que le permite renovar de forma automática su certificado.

- El empleo del certificado vigente para su renovación, en los términos legalmente establecidos.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2 Validación para la renovación de certificados tras la revocación

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado, la Entidad de Certificación de la OMC comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

3.4 Identificación y autenticación de la solicitud de revocación

La Entidad de Certificación de la OMC autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor, firmada electrónicamente.
- El uso de la "frase de comprobación de identidad", que consiste en información que sólo conoce el poseedor de claves, y que le permite revocar de forma automática su certificado.

- La personación física en una oficina de un Colegio de Médicos o para un médico externo a su Servicio Autonómico de Salud.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de la Entidad de Certificación de la OMC.

3.5 Autenticación de una petición de suspensión

La petición de suspensión se realizará por el suscriptor utilizando el formulario existente en la web de la ECOMC (https://certificacion.cgcom.es) para dicho cometido en horario de 24x7.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación ya sea presencialmente o por teléfono en el Colegio de Médicos, CGCOM o Servicio Autonómico de Salud y existan dudas para su identificación, su certificado pasa a estado de suspensión.

4 Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud de emisión de certificado

4.1.1 Legitimación para solicitar la emisión

Antes de la emisión y entrega de un certificado, existe una solicitud de certificado, que puede producirse de oficio o a instancia de parte interesada.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por el Colegio profesional, una Entidad del ámbito santiario o el Servicio Autonómico de Salud.

4.1.2 Procedimiento de alta; Responsabilidades

Existen los siguientes tipos de solicitudes:

1) Solicitud electrónica de certificado de oficio (no contiene clave pública, ni se encuentra firmada digitalmente).
2) Solicitud electrónica de certificado de parte sin generación de claves (no contiene clave pública, ni se encuentra firmada digitalmente).

La Entidad de Certificación de la OMC recibe solicitudes de certificados, realizadas de oficio por las entidades que integran la Organización Médica Colegial, o por una Entidad del ámbito sanitario o por el Servicio Autonómico de Salud, o a instancia de parte.

En el primer caso existe un documento, ya sea en soporte papel o en formato electrónico, referente a la solicitud de certificados, realizada por el Colegio, Entidad del ámbito sanitario o el Servicio Autonómico de Salud a la Entidad de certificación, el cual incluirá la indicación de la persona o personas a autorizar para realizar peticiones, así como, en su caso, los datos de las personas a las que se expedirán certificados.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias del poseedor de claves, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar al poseedor de claves.

Asimismo, el Colegio, la Entidad del ámbito sanitario o el Servicio Autonómico de Salud acepta un convenio de suscriptor, en forma de condiciones generales de emisión.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, la Entidad de Certificación de la OMC se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, la Entidad de Certificación de la OMC verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2.

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud ha de conservar debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso todo en caso de pérdida anticipada de vigencia por revocación.

El plazo de conservación de la documentación acreditativa de la solicitud de certificados no cualificados no podrá ser inferior a 5 años desde la expiración del certificado.

4.2.2 Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la Entidad de Certificación de la OMC debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, la Entidad de Certificación de la OMC deniega la petición, o detiene su

aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, se deniega la solicitud definitivamente.
La Entidad de Certificación notifica al solicitante la aprobación o denegación de la solicitud.

4.2.3 Plazo para resolver la solicitud

La Entidad de Certificación de la OMC atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.
Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3 Emisión del certificado

4.3.1 Acciones de la Entidad de Certificación de la OMC durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado y, cuando sea necesario, grabación en la tarjeta, de forma segura y se pone la misma a disposición del suscriptor, que la entrega al poseedor de claves para su aceptación, de acuerdo con lo establecido en la sección 4.3.2.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

La Entidad de Certificación de la OMC:
- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves, y, cuando sea necesario, almacena la clave privada de forma segura y el correspondiente certificado en la tarjeta del poseedor de claves.

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de 19 de diciembre, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1.
- Indica la fecha y la hora en que se expidió un certificado.
- Cuando se utilitza una tarjeta criptográfica, se emplea un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al suscriptor.

Los procesos de emisión técnica del certificado y de impresión segura, manipulado y, cuando sea necesario, envío de las tarjetas a los Colegios suscriptores, así como de los datos de identificación y acceso a los poseedores, se encuentran subcontratados a terceras entidades, mediante los oportunos contratos de encargo de tratamiento de datos personales y bajo la plena responsabilidad de la Entidad de Certificación de la OMC.

4.3.2 Notificación de la emisión al suscriptor

La Entidad de Certificación de la OMC notifica la emisión del certificado al suscriptor y al poseedor de claves.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades de la Entidad de Certificación de la OMC

La Entidad de Certificación:

- Acredita definitivamente la identidad del poseedor de claves, con la colaboración del Colegio, la Entidad del ámbito sanitario o el Servicio Autonómico de Salud suscriptor, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Entrega al poseedor de claves, con la colaboración del Colegio, la Entidad del ámbito sanitario o el Servicio Autonómico de Salud suscriptor, cuando sea necesario, la tarjeta que contiene el certificado.
- Entrega al poseedor de claves, con la colaboración del Colegio, la Entidad del ámbito sanitario o el Servicio Autonómico de Salud suscriptor, una hoja de entrega y aceptación

del certificado, y cuando sea necesario también de la tarjeta, con los siguientes contenidos mínimos:

a) Información básica acerca de la política y uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades

b) Información acerca del certificado y, cuando sea necesario, de la tarjeta.

c) Reconocimiento por parte del poseedor, de recibir el certificado y cuando pertoque de la tarjeta, y la aceptación de los citados elementos.

d) Obligaciones del poseedor de claves.

e) Responsabilidad del poseedor de claves.

f) Método de imputación exclusiva al poseedor de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones 6.2 y 6.4.

g) La fecha del acto de entrega y aceptación.

El suscriptor colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y remitir los citados documentos originales a la Entidad de Certificación de la OMC.
Para ello, la Entidad de Certificación de la OMC remite al suscriptor el paquete de tarjetas solicitadas, junto con las hojas de entrega y aceptación correspondientes, y remite directamente a cada poseedor de claves sus datos de activación de firma y otras informaciones.

Las tarjetas se entregan protegidas, de forma que únicamente el poseedor de claves puede hacer uso de las mismas.

4.4.2 Conducta que constituye aceptación del certificado

La aceptación del certificado por el poseedor de claves se produce mediante la firma de la hoja de entrega y aceptación ante el Colegio, la Entidad jurídica del ámbito sanitario o el Servicio Autonómico de Salud suscriptor.

Cuando el poseedor de claves ha aceptado el certificado y, en su caso, la tarjeta, puede con los datos de activación recibidos y producir firmas electrónicas.

Una vez entregado o descargado el certificado, el usuario dispone de un periodo de 7 días para comprobar su correcto funcionamiento.

4.4.3 Publicación del certificado

La Entidad de Certificación de la OMC publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.4.4 Notificación de la emisión a terceros

La Entidad de Certificación de la OMC no realiza ninguna notificación de la emisión a terceras entidades.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el suscriptor

4.5.1.1 Obligaciones del suscriptor del certificado

La Entidad de Certificación de la OMC obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Reconocer su capacidad de producción de firmas electrónicas reconocidas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4.
- Comunicar a la Entidad de Certificación y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  a) La pérdida, el robo o el compromiso potencial de su clave privada.
  b) La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.

c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

d) La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.

- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.
- Imponer a los poseedores de claves el cumplimiento de las obligaciones específicas de los mismos.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Entidad de Certificación de la OMC, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación del prestador de servicios de certificación de la Entidad de Certificación de la OMC, sin permiso previo por escrito.

4.5.1.2 Responsabilidad civil del suscriptor de certificado

La Entidad de Certificación de la OMC obliga contractualmente al suscriptor a garantizar:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del suscriptor, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni a título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2 Uso por el tercero que confía en certificados

4.5.2.1 Obligaciones del tercero que confía en certificados

La Entidad de Certificación obliga contractualmente al tercero que confía en certificados a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en tarjeta, tienen la consideración legal de firmas electrónicas reconocidas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Entidad de Certificación de la OMC, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Entidad de Certificación de la OMC, sin permiso previo por escrito.

4.5.2.2 Responsabilidad civil del tercero que confía en certificados

La Entidad de Certificación de la OMC obliga contractualmente al suscriptor a manifestar:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6 Renovación de certificados

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 4.7.

4.7 Renovación de claves y certificados

4.7.1 Causas de renovación de claves y certificados

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

4.7.2 Legitimación para solicitar la renovación

Antes de la emisión y entrega de un certificado renovado, existe una solicitud de renovación de certificado, que puede producirse de oficio o a instancia de parte interesada.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por el Colegio profesional o el Servicio Autonómico de Salud.

4.7.3 Procedimientos de solicitud de renovación

4.7.3.1 Realización de la solicitud

La Entidad de Certificación de la OMC recibe solicitudes de certificados, realizadas de oficio por las entidades que integran la Organización Médica Colegial, o una Entidad jurídica del ámbito sanitario o el Servicio Autonómico de Salud, o a instancia de parte.

En el primer caso existe un documento, ya sea en soporte papel o en formato electrónico, referente a la solicitud de renovación de certificados, realizada por el Colegio, la Entidad jurídica del ámbito sanitario o el Servicio Autonómico de Salud a la Entidad de certificación, el cual incluirá la indicación de la persona o personas a autorizar para realizar peticiones, así como, en su caso, los datos de las personas a las que se expedirán certificados.

La solicitud ha de indicar que los datos de los certificados no han cambiado, pudiendo únicamente indicar cambios en la dirección física, u otros datos, que permitan contactar al poseedor de claves.

Asimismo, el Colegio, la Entidad jurídica del ámbito sanitario o Servicio Autonómico de Salud acepta un convenio de suscriptor, en forma de condiciones generales de emisión.

4.7.3.2 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de renovación de certificado, la Entidad de Certificación de la OMC se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

4.7.3.3 Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la Entidad de Certificación debe aprobar la solicitud de renovación del certificado y proceder a su emisión y entrega.

La Entidad de Certificación notifica al solicitante la aprobación o denegación de la solicitud.

4.7.3.4 Plazo para resolver la solicitud

La Entidad de Certificación de la OMC atiende las solicitudes de renovación certificados por orden de llegada, en un plazo razonable anterior a la expiración de los certificados a revocar, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.
Las solicitudes de renovación se mantienen activas hasta su aprobación o rechazo.

4.7.4 Notificación de la emisión del certificado renovado

La Entidad de Certificación de la OMC notifica la emisión del certificado al suscriptor y al poseedor de claves.

4.7.5 Conducta que constituye aceptación del certificado

La aceptación del certificado por el poseedor de claves se produce mediante la firma de la hoja de entrega y aceptación ante el suscriptor.

Cuando el poseedor de claves ha aceptado el certificado y, cuando sea necesario, la tarjeta, puede con los datos de activación recibidos producir firmas electrónicas.

4.7.6 Publicación del certificado

La Entidad de Certificación de la OMC publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.7 Notificación de la emisión a terceros

La Entidad de Certificación de la OMC no realiza ninguna notificación de la emisión a terceras entidades.

4.8 Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada - que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.9 Revocación y suspensión de certificados

Esta sección detalla las prácticas relativas a la revocación y suspensión de certificados.

4.9.1 Causas de revocación de certificados

La Entidad de Certificación de la OMC revoca un certificado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:

a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.

b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.

c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:

a) Compromiso de la clave privada o de la infraestructura o sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b) Infracción, por la Entidad de certificación de la OMC, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.

d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.

e) El uso irregular del certificado por el poseedor de claves, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan a la seguridad de la tarjeta:

a) Compromiso o sospecha de compromiso de la seguridad de la tarjeta.

b) Pérdida o inutilización por daños de la tarjeta.

c) Acceso no autorizado, por un tercero, a los datos de activación del poseedor de claves.

4) Circunstancias que afectan al suscriptor o al poseedor de claves:

a) Finalización de la relación jurídica de prestación de servicios entre la Entidad de Certificación de la OMC y el suscriptor.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al poseedor de claves.

c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción por el suscriptor o por el poseedor de claves, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y poseedor de claves.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

5) Otras circunstancias:

a) La terminación del servicio de certificación de la OMC, de acuerdo con lo establecido en la sección 5.8.

b) El uso del certificado que sea dañino y continuado para la OMC o Camerfirma . En este caso, se considera que un uso es dañino en función de los siguientes criterios:

1º) La naturaleza y el número de quejas recibidas.

2º) La identidad de las entidades que presentan las quejas.

3º) La legislación relevante vigente en cada momento.

4º) La respuesta del suscriptor o del poseedor de claves a las quejas recibidas.

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- El propio poseedor de claves.
- Un representante autorizado por el suscriptor.
- La Entidad de Certificación de la OMC, así como sus colaboradores en las tareas de registro y emisión.

4.9.3 Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo a la Entidad de Certificación de la OMC o, en su caso, al Colegio, el Servicio Autonómico de Salud o el registrador que tramitó la solicitud de certificación, comprensiva de la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

La solicitud debe ser autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

El servicio de revocación se encuentra en la página de la Web de la EC OMC en la siguiente dirección:
https://certificacion.cgcom.es/revocar_certificado

En caso de que el destinatario de una solicitud de revocación por parte de un poseedor de claves fuera el Colegio, la Entidad jurídica del ámbito sanitario o el Servicio Autonómico de Salud suscriptor, una vez autenticada la solicitud debe remitir una solicitud en este sentido a la Entidad de Certificación de la OMC.

La solicitud de revocación será procesada a su recepción.

Se informa al suscriptor y, en su caso, al poseedor de claves, acerca del cambio de estado del certificado revocado.

La Entidad de Certificación de la OMC no reactiva el certificado, una vez ha sido revocado.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de la EC OMC y AC Camerfirma.

4.9.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación.

4.9.5 Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, dentro del horario ordinario de operación de la Entidad de Certificación de la OMC.

4.9.6 Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de la OMC. El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación de la OMC, así como en las siguientes direcciones web, indicadas dentro de los certificados:

http://crl3.cgcom.es/crl/eccgcom.crl
http://crl4.cgcom.es/crl/eccgcom.crl

Otro método es la consulta de un servicio web que comunica los certificados revocados, según se indica posteriormente.

4.9.7 Frecuencia de emisión de listas de revocación de certificados (LRCs)

La Entidad de Certificación de la OMC emite una LRC al menos cada 24 horas.

La EC OMC y AC Camerfirma emiten y publican **listas de revocados** de forma periódica siguiendo la siguiente tabla, e inmediatamente después de producirse una revocación.

CHAMBERSIGN ROOT - 2008	365 días	365 días
AC CAMERFIRMA	180 días	180 días
EC OMC	24 horas	48 horas

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

4.9.8 Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediatamente razonable, tras su generación, que no supera unos pocos minutos en ningún caso.

4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de la Entidad de Certificación de la OMC, que se encuentra disponible las 24 horas de los 7 días de la semana.

La dirección electrónica del Depósito es:
https://www.cgcom.es/deposito

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *AC ROOT de Chambersign de Camerfirma*
    - http://crl.chambersign.org/chambersroot.crl
- *AC Camerfirma intermedia:*
    - http://crl.camerfirma.com/ac_camerfirma-2009.crl
- *EC-OMC:*
    - https://certificacion.cgcom.es/infoacomc/crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Entidad de Certificación de la OMC, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

La Entidad de Certificación de la OMC suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

El tercero que confía en el certificado que no emplee LRCs para comprobar la validez de un certificado, debe emplear el Depósito o el servicio web para ello.

4.9.11 Otras formas de información de revocación de certificados

La Entidad de Certificación de la OMC también informa acerca del estado de revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados en linea desde la dirección siguiente:
http://ocsp.cgcom.es

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de la Entidad de Certificación de la OMC es notificado, en la medida de lo posible, a todos los participantes en los servicios de certificación de la OMC,

mediante la publicación de este hecho en la página web de la OMC, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.13 Causas de suspensión de certificados

Los certificados de la Entidad de Certificación de la OMC pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente, aunque se pueda identificar razonablemente al suscriptor.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente y tampoco permitan identificar razonablemente al suscriptor.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, la Entidad de Certificación de la OMC tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.9.14 Solicitud de suspensión

Pueden solicitar la suspensión del certificado:

- El poseedor de claves del certificado (médico, personal administrativo, etc)
- El suscriptor del certificado (Colegio de Médicos, Servicio Autonómico de Salud, etc)
- La Entidad de Certificación de la OMC

4.9.15 Procedimientos para la petición de suspensión

- El usuario accede a un formulario web que se encuentra en la web de la Entidad de Certificación de la OMC (https://certificacion.cgcom.es)
- Una vez rellenado el formulario con su número y letra de DNI/NIE, se envía un password temporal al correo electrónico con el que el usuario solicitó el certificado.
- El usuario debe confirmar con ese password su solicitud de suspensión.

- Una vez confirmada la solicitud, la Entidad de Certificación de la OMC procede a la suspensión del certificado.

4.9.16 Período máximo de suspensión

El plazo máximo de suspensión será de una semana.

4.10 Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

La Entidad de Certificación de la OMC puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11 Servicios de comprobación de estado de certificados

4.11.1 Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, a través del Depósito de los certificados, y mediante un servicio web específico de consulta.

4.11.2 Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.11.3 Características opcionales

Los servicios de comprobación de estado de certificados no presentan características opcionales.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

La Entidad de Certificación de la OMC no presta servicios de depósito y recuperación de claves.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5 Controles de seguridad física, de gestión y de operaciones

En este apartado diferenciaremos dominios de actuación de la Entidad de Certificación de la Organización Médica Colegial.

De esta forma podemos encontrar:

Dominio de creación de certificados.
Los controles de seguridad física, de gestión y de operaciones en el dominio de creación de los certificados son operados por la entidad Camerfirma y se realizan de acuerdo con las indicaciones de la CPS de la Global Chambersign Root-2008. Camerfirma cumple con los controles declarados en esta DPC.
La Autoridad de Certificación Camerfirma que da soporte a las operaciones de gestión de certificados de la EC OMC está sujeta a las validaciones anuales de la norma ISO/IEC 27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna
Los controles de seguridad física, de gestión y de operaciones en el dominio del registro de los usuarios y, cuando sea necesario, la gestión de tarjetas criptográficas son operados por una entidad u organización perteneciente a la OMC (por ejemplo un Colegio de Médicos), o por un Servicio Autonómico de Salud o una Entidad del ámbito sanitario.

5.1 Controles de seguridad física

Dominio de creación de certificados

La Entidad de Certificación de la OMC, por medio de Camerfirma, ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se

encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de generación técnica de los certificados.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados, actividad que se encuentra subcontratada a AC Camerfirma, bajo la plena responsabilidad de la Entidad de Certificación de la OMC, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia **24h-365** días al año con asistencia en las **24 horas** siguientes al aviso

Dominio de registro de usuarios y gestión de tarjetas por entidad interna

La Entidad de Certificación de la OMC, en las instalaciones de una entidad interna, ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes de certificados, así como de la gestión de las tarjetas criptográficas de médicos colegiados.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de registro y aprobación de las solicitudes de certificados, así como de la gestión, cuando sea necesario, de las tarjetas criptográficas, ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección antirrobos.
- Allanamiento y entrada no autorizada.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones de la entidad interna donde se realiza la aprobación de las solicitudes de certificados y, cuando sea necesario, la gestión de las tarjetas criptográficas bajo la plena responsabilidad de la Entidad de Certificación de la OMC.

La Entidad de Certificación de la OMC, en las instalaciones de la entidad interna, ha establecido medidas de seguridad y de protección de datos personales suficientes en relación con los servicios de aprobación y de generación técnica y de manipulado de tarjetas.

5.1.1 Localización y construcción de las instalaciones

Dominio de creación de certificados
La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.
En concreto, la sala donde se realizan las operaciones criptográficas es una caja de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.La Entidad de Certificación de la OMC, en las instalaciones de la entidad

interna dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados, de gestión –cuando sea necesario- de tarjetas y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

5.1.2 Acceso físico

Dominio de creación de certificados

La Entidad de Certificación de la OMC, en las instalaciones de la subcontratada AC CAmerfirma, dispone de un mínimo de cuatro niveles de seguridad física (Edificio, Oficinas, CPD y Sala criptográfica) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de AC Camerfirma donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

El acceso a los elementos más críticos del sistema se realiza a través de tres zonas previas de paso con acceso limitado incrementalmente.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna

La Entidad de Certificación de la OMC, en las instalaciones de la entidad interna, dispone de la adecuada y suficiente seguridad física para la protección del servicio de aprobación de las solicitudes de certificados y de gestión, cuando sea necesario, de las tarjetas criptográficas.

5.1.3 Electricidad y aire acondicionado

Dominio de creación de certificados

Las instalaciones de la EC OMC provistas por AC Camerfirma disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 Exposición al agua

Dominio de creación de certificados

La Entidad de Certificación de la OMC, en las instalaciones de la subcontratada AC Camerfirma, están ubicadas en una zona de bajo riesgo de inundación. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Dominio de creación de certificados

Todas las instalaciones y activos de la Entidad de Certificación de la OMC, en las instalaciones de Camerfirma, cuentan con sistemas automáticos de detección y extinción de incendios.

Los dispositivos criptográficos, y soportes que almacenen claves de las Entidades de Certificación, cuentan con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

Dominio de registro de usuarios y gestión, cuando sea necesario, de tarjetas por entidad interna

Todas las instalaciones y activos de la Entidad de Certificación de la OMC, en las instalaciones de las entidades internas, cuentan con sistemas de extinción de incendios, de acuerdo con las normativas locales de prevención de incendios.

5.1.6 Almacenamiento de soportes

Dominio de creación de certificados

Cada Medio de Almacenamiento desmontable (cintas, cartuchos, disquetes, etc.) permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento se guarda en armarios ignífugos o bajo llave permanentemente en requiriéndose autorización expresa para su retirada.

5.1.7 Tratamiento de residuos

Dominio de creación de certificados

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control..

5.1.8 Copia de respaldo fuera de las instalaciones

Dominio de creación de certificados

La EC OMC utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro operacional.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2 Controles de procedimientos

Dominio de creación de certificados

La Entidad de Certificación de la OMC garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de la Entidad de Certificación de la OMC ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

Dominio de creación de certificados

La Entidad de Certificación de la OMC, en las instalaciones de la subcontratada AC Camerfirma, ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- Auditor Interno: Responsable del cumplimiento de los procedimientos operativos. Es una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- Administrador de Sistemas: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- Administrador de AC: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- Operador de AC: Responsable necesario conjuntamente con el Administrador de AC de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de backup y mantenimiento de la AC.
- Administrador de AR: Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor.
- Responsable de Seguridad: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de la EC OMC. Debe

encargarse aspecto relacionado con la seguridad del información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.

Dominio de registro de usuarios y gestión, cuando sea necesario, de tarjetas por entidad interna

La Entidad de Certificación de la OMC, por medio de la entidad interna, ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- Personal de atención al cliente.
- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.

5.2.2 Número de personas por tarea

Dominio de creación de certificados

La EC OMC garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes. Principalmente en la manipulación del dispositivo de custodia de las claves de AC Root y AC intermedias.

5.2.3 Identificación y autenticación para cada función

Dominio de creación de certificados

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.
El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

5.2.4 Roles que requieren separación de tareas

Dominio de creación de certificados
Las siguientes tareas son realizadas, al menos, por dos personas:
- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

5.2.5 Arranque y parada del sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Módulo de Gestión de AR, para lo cual se activaran o desactivaran los servicios del gestor de páginas especifico. Actualmente AC la OMC gestiona dos plataformas técnicas distintas para cada una de las jerarquías, aunque el apagado se realiza de la misma forma desactivando los servicios del gestor de páginas.
- Módulo de gestión de solicitudes, para lo cual se activara o desactivara los servicios del gestor de páginas específico.
- Módulo de gestión de claves, ubicado en el equipo HSM. Se activa o desactiva mediante encendido físico.
- Módulo de BBDD, Gestión centralizada de los certificados y CRL gestionados, OCSP y TSA. Arranque y parada del servicio específico del Gestor de BBDD.
- Módulo OCSP. Servidor de respuestas de estado de los certificados en línea. Arranque y parada del servicio de sistema encargado de esta tarea.
- Módulo TSA. Servidor de sellos de tiempos. Arranque y parada del servicio

El proceso de apagado de módulos seguiría la secuencia:

- Módulo de solicitud
- Módulo de AR
- Módulo OCSP
- Módulo TSA

- Módulo BBDD
- Módulo gestión de claves.

Se realizará el encendido en proceso inverso.

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Dominio de creación de certificados

Todo el personal que realiza tareas calificadas como confiables, lleva al menos **un año** trabajando en el centro de producción y tiene contratos laborales fijos.
Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.
El personal en puestos de confianza se encontrará libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.
La EC OMC se asegura de que el personal de registro o Administradores de AR es confiable y pertenece a los Colegios Oficiales de Médicos o del organismo delegado para realizar las tareas de registro.
El Administrador de AR habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones.
En general, la EC OMC retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.
La EC OMC no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación, hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad

5.3.2 Procedimientos de investigación de historial

Dominio de creación de certificados

La Entidad de Certificación de la OMC, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

La EC OMC obtiene consentimiento inequívoco del afectado por la investigación previa y procesa y protege todos sus datos personales de acuerdo con la LOPD y el REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente en cada momento y lugar. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

5.3.3 Requisitos de formación

Dominio de creación de certificados

La Entidad de Certificación forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.
Los programas de formación son actualizados y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de la Entidad de Certificación de la OMC. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4 Requisitos y frecuencia de actualización formativa

Dominio de creación de certificados

La Entidad de Certificación de la OMC, actualiza la formación del personal de acuerdo con las necesidades y la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

Dominio de creación de certificados

La Entidad de Certificación de la OMC dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7 Requisitos de contratación de profesionales

Dominio de creación de certificados

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y la requerimientos operacionales empleados por la EC OMC. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución.

Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a la EC OMC.

5.3.8 Suministro de documentación al personal

Dominio de creación de certificados

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4 Procedimientos de auditoria de seguridad

La Autoridad de Certificación Camerfirma bajo la que se establece la EC OMC está sujeta a las validaciones anuales de la norma ISO/IEC 27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información que dan soporte a los procesos de certificación electrónica.

5.4.1 Tipos de eventos registrados

Dominio de creación de certificados

La Entidad de Certificación de la OMC produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

Se registraran los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este

La EC OMC, por medio de AC Camerfirma, también conserva, ya sea manualmente o electrónicamente, la siguiente información

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por

5.4.2 Frecuencia de tratamiento de registros de auditoría

Dominio de creación de certificados

La EC OMC, junto con AC Camerfirma, revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

La EC OMC, junto con AC Camerfirma, mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardaran en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3 Periodo de conservación de registros de auditoría

Dominio de creación de certificados

La EC OMC, junto con AC Camerfirma, almacena la información de los logs al menos durante **5 años**.

5.4.4 Protección de los registros de auditoría

Dominio de creación de certificados

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas.

Los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5 Procedimientos de copia de respaldo

Dominio de creación de certificados

La EC OMC, junto con AC Camerfirma, dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

La EC OMC, junto con AC Camerfirma, tiene implementado un procedimiento de back up seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo.

Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6 Localización del sistema de acumulación de registros de auditoría

Dominio de creación de certificados

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, la comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado, todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación del evento de auditoria al causante del evento

Dominio de creación de certificados

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8 Análisis de vulnerabilidades

Dominio de creación de certificados

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de la EC OMC, junto con AC Camerfirma.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente.
Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5 Archivo de informaciones

Para todos los dominios
La Entidad de Certificación de la OMC, garantiza que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1 Tipos de registros archivados

Dominio de creación de certificados
Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la AC o por las AR's:

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación

La EC OMC es responsable del correcto archivo de todo este material.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
La Entidad de Certificación de la OMC, en las instalaciones de la subcontratada o de la entidad interna, archiva:

- Todos los datos de auditoría identificados en la sección 5.4.

- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

5.5.2 Periodo de conservación de registros

Para todos los dominios

La Entidad de Certificación de la OMC archiva los registros especificados anteriormente durante 15 años.

5.5.3 Protección del archivo

Para todos los dominios

La Entidad de Certificación de la OMC protege el archivo de forma que sólo personas fiables debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

La EC OMC asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

5.5.4 Procedimientos de copia de respaldo

Dominio de creación de certificados

La EC OMC, junto con AC Camerfirma, dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

La EC OMC, junto con AC Camerfirma, como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

La Entidad de Certificación de la OMC, en las acciones realizadas por la subcontratada o por la entidad interna, realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, y copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, la Entidad de Certificación, en la entidad interna, guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5 Requisitos de sellado de fecha y hora

Dominio de creación de certificados
Los registros están fechados con una fuente fiable vía NTP desde el ROA, GPS y sistemas de sincronización vía Radio.
La EC OMC dispone de un documento de seguridad informática donde describe la configuración de tiempos de los equipos utilizados en la emisión de certificados.
No es necesario que esta información se encuentre firmada digitalmente.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
Las bases de datos de la Entidad de Certificación emplean registros fiables de fecha y hora.
No es necesario que esta información se encuentre firmada digitalmente.

5.5.6 Localización del sistema de archivo

Dominio de creación de certificados
La EC OMC dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Dominio de creación de certificados
La EC OMC dispone de un documento de seguridad informática donde se describe el proceso para verificar que la información archivada es correcta y accesible.

5.6 Renovación de claves

Dominio de creación de certificados

La renovación de las claves de la Entidad de Certificación de la OMC, en las instalaciones de la subcontratada Camerfirma, se realiza de acuerdo con los procedimientos descritos en la declaración de prácticas de certificación de la Root AC Global Chambersign Root – 2008, de Camerfirma..

Antes de que el uso de la clave privada de la AC caduque se realizará un cambio de claves. La vieja AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por la AC vieja. Se generará una nueva AC con una clave privada nueva y un nuevo DN.
El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

No aplicable

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimientos de gestión de incidencias y compromisos

Dominio de creación de certificados

Se guardan copias de seguridad de la siguiente información de la Entidad de Certificación, en instalaciones de almacenamiento externo a la Entidad de Certificación, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de la Entidad de Certificación son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4.

Dominio de registro de usuarios y gestión de tarjetas por entidad interna.

Se guardan copias de seguridad de la siguiente información de la Entidad de Certificación, en instalaciones de almacenamiento externo a la Entidad de Certificación, que se ponen a disposición en caso de compromiso o desastre: datos de solicitud de certificados.

5.7.2 Corrupción de recursos, aplicaciones o datos

Dominio de creación de certificados

Cuando ocurre un evento de corrupción de recursos, aplicaciones o datos, se comunica la incidencia a seguridad y se inician los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se inician los procedimientos de compromiso de claves o de recuperación de desastres de la Entidad de Certificación de la OMC, en las instalaciones de la subcontratada Symantec,.

5.7.3 Compromiso de la clave privada de la entidad

Dominio de creación de certificados

En caso de sospecha o conocimiento del compromiso de la Entidad de Certificación de la OMC, se activan los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evalúa la situación, desarrolla un plan de acción y lo ejecuta con la aprobación de la dirección de la Entidad de Certificación.

La Autoridad de Certificación de Camerfirma que da soporte a las operaciones de EC OMC ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario un centro de datos alternativo.
El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratara los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.
Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

No aplicable para este ámbito.

5.7.4 Continuidad del negocio después de un desastre

Dominio de creación de certificados

La EC OMC, junto con AC Camerfirma, restablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con el plan de contingencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.
La Autoridad de Certificación de Camerfirma que da soporte a las operaciones de gestión de certificados de EC OMC dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descrito en el plan de continuidad de negocio.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
No aplicable para este ámbito.

5.8 Terminación del servicio

Dominio de creación de certificados

La Entidad de Certificación de la OMC, en las instalaciones de la subcontratada AC Camerfirma, asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, la Entidad de Certificación desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de **6 meses**.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá 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.
- Las claves privadas de la AC serán destruidas o deshabilitadas para su uso.
- La EC OMC o AC Camerfirma mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

La Entidad de Certificación de la OMC, en las instalaciones de la entidad interna, asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, la Entidad de Certificación, en la entidad interna, desarrolla un plan de terminación, con las siguientes provisiones:

- Ejecución de las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.

6 Controles de seguridad técnica

La Entidad de Certificación de la OMC emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de la Entidad de la Certificación de la OMC es creado por la Entidad de Certificación subordinada AC Camerfirma-2009, de acuerdo con los procedimientos de ceremonia de claves de la Global Chambersign Root-2008, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves son registradas, fechadas y firmadas por todos los individuos participantes en la misma. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un periodo apropiado determinado por Camerfirma.

Para la generación de la clave de la SubCA se utiliza un dispositivo que cumple los requerimientos que se detallan en el **FIPS 140-2 de nivel 3**. Se disponen de HSM con la misma certificación para la emisión de respuestas OCSP y sellos de tiempo.
Las claves Raíz e intermedias fueron generadas en respectivas ceremonias de las que hay documentación detallada.

AC ROOT-Chambersign Global Root 2008	**4.096 bits**	**30 Años**
SUBCA CONSEJO GENERAL DE COLEGIOS DE MÉDICOS DE ESPAÑA	**4.096 bits**	**10 Años**
Certificado corporativo de colegiado (persona física) para identificación	2.048 bits	5 Años
Certificado corporativo de colegiado (persona física) para firma	2.048 bits	5 Años

Certificado corporativo de colegiado (persona física) para cifrado	2.048 bits	5 Años
Certificado corporativo de colegiado (persona física), en SOFTWARE, para identificación, firma y cifrado	2.048 bits	5 Años
Certificado corporativo de colegiado (persona física), en HSM, para identificación, firma y cifrado	2.048 bits	5 Años
Certificado corporativo de personal administrativo (persona física) para identificación	2.048 bits	5 Años
Certificado corporativo de personal administrativo (persona física) para firma	2.048 bits	5 Años
Certificado de cifrado en tarjeta, para personal administrativo	2.048 bits	5 Años
Certificado corporativo de personal administrativo (persona física), en software, para identificación, firma y cifrado	2.048 bits	5 Años
Certificado corporativo de persona jurídica para identificación	2.048 bits	5 Años
Certificado corporativo de persona jurídica para firma	2.048 bits	5 Años
Certificado de cifrado en tarjeta, para persona jurídica	2.048 bits	5 Años
Certificado corporativo de persona jurídica en software, para identificación, firma y cifrado	2.048 bits	5 Años
Certificado de colectivo de médico empleado público (persona física) para identificación	2.048 bits	5 Años
Certificado de colectivo de médico empleado público (persona física) para firma	2.048 bits	5 Años
Certificado de cifrado en tarjeta, para médico empleado público	2.048 bits	5 Años

Más información en las siguientes direcciones web:

Certificado corporativo de colegiado (persona física) para identificación	https://www.cgcom.es/CertCol

Certificado corporativo de colegiado (persona física) para firma	
Certificado corporativo de colegiado (persona física) para cifrado	
Certificado corporativo de colegiado (persona física), en SOFTWARE, para identificación, firma y cifrado	https://www.cgcom.es/CertColSoft
Certificado corporativo de colegiado (persona física), en HSM, para identificación, firma y cifrado	https://www.cgcom.es/CertColHSM
Certificado corporativo de personal administrativo (persona física) para identificación	https://www.cgcom.es/CertAdmin
Certificado corporativo de personal administrativo (persona física) para firma	
Certificado de cifrado en tarjeta, para personal administrativo	
Certificado corporativo de personal administrativo (persona física), en software, para identificación, firma y cifrado	https://www.cgcom.es/CertAdminSoft
Certificado corporativo de persona jurídica para identificación	https://www.cgcom.es/CertJur
Certificado corporativo de persona jurídica para firma	
Certificado de cifrado en tarjeta, para persona jurídica	
Certificado corporativo de persona jurídica en software, para identificación, firma y cifrado	https://www.cgcom.es/CertJurSoft
Certificado de colectivo de médico empleado público (persona física) para identificación	https://www.cgcom.es/CertMEP
Certificado de colectivo de médico empleado público (persona física) para firma	
Certificado de cifrado en tarjeta, para médico empleado público	

6.1.1.1 Generación del par de claves del suscriptor

Las claves del Firmante/Suscriptor pueden ser creadas en por el mismo mediante dispositivos hardware o software autorizados por la EC OMC o pueden ser creadas por la EC OMC en formato software **PKCS#12.**
Las claves son generadas usando el algoritmo de clave pública **SHA**.
Las claves Tienen una longitud mínima de **2048 bits**.
En el caso de que el suscriptor genere las claves en un dispositivo criptográfico propio. La EC OMC exigirá un informe técnico de auditoría que valorará antes de emitir un certificado marcado con claves generadas en dispositivo hardware. Si el suscriptor no aportara el documento o no fuera satisfactorio la EC OMC solo estaría en condiciones de emitir un certificado catalogado como claves generadas en dispositivo software.

6.1.2 Envío de la clave privada al suscriptor

En certificados en tarjeta criptográfica
La clave privada del suscriptor se le entrega debidamente protegida mediante la entrega de la tarjeta criptográfica indicada anteriormente.

La preparación de la tarjeta es controlada de forma segura por la Entidad de Certificación de la OMC. La tarjeta es almacenada y distribuida de forma segura por la Entidad de Certificación de la OMC, como se indica en la sección 4.4, y la desactivación y reactivación de la tarjeta se controla de forma segura.

En certificados en software
La clave privada del suscriptor se crea en el sistema informático que utiliza el suscriptor, cuando realiza la solicitud de certificado, por lo que en este caso no existe envío de clave privada.

6.1.3 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por la Organización Médica Colegial.

6.1.4 Distribución de la clave pública del prestador de servicios de certificación

Las claves de la Entidad de Certificación de la OMC son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de la AC y su fingerprint (huella digital) estarán a disposición de los usuarios en la página Web de la EC OMC

6.1.5 Tamaños de claves

La longitud de las claves de la Entidad de Certificación de la OMC es de 4096 bits.
Las claves de los subscriptores de certificados son de 2048 bits, a partir del 1 de Mayo de 2011.

6.1.6 Generación de parámetros de clave pública

La clave pública de la AC Raíz y de la AC Subordinada y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

6.1.7 Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 2048
- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-1, SHA256.

6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9 Propósitos de uso de claves

En el siguiente grafico se describe los usos de la clave para los distintos certificados emitidos. La solución adoptada para la diferenciación de usos es la siguiente:

Certificados para autenticación bit DS (puede convivir con otros usos)
Certificados para firma electrónica bit DS + NR (puede convivir con otros usos)
Certificados exclusivos de firma reconocida bit NR (NO puede convivir con otros usos).

Leyenda:
DS Firma Digital
NR No Repudio, "ContentCommitment"
KE Cifrado de Clave
DE Cifrado de Datos
KA Acuerdo de clave
KCS Firma de certificados
CRL Firma de CRL
EO Solo Cifrado
DO Solo descifrado

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
AC ROOT -Chambersign Global Root						X	X		
SUBCA CONSEJO GENERAL DE COLEGIOS DE MÉDICOS DE ESPAÑA						X	X		
Certificado corporativo de colegiado (persona física) para identificación	X								
Certificado corporativo de colegiado (persona física) para firma		X							

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
Certificado corporativo de colegiado (persona física) para cifrado			X	X					
Certificado corporativo de colegiado (persona física), en SOFTWARE, para identificación, firma y cifrado	X	X	X	X					
Certificado corporativo de colegiado (persona física), en HSM, para identificación, firma y cifrado	X	X	X	X					
Certificado corporativo de personal administrativo (persona física) para identificación	X								
Certificado corporativo de personal administrativo (persona física) para firma		X							
Certificado de cifrado en tarjeta, para personal administrativo			X	X					
Certificado corporativo de personal administrativo (persona física), en software, para identificación, firma y cifrado	X	X	X	X					
Certificado corporativo de persona jurídica para identificación	X								

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
Certificado corporativo de persona jurídica para firma		X							
Certificado de cifrado en tarjeta, para persona jurídica			X	X					
Certificado corporativo de persona jurídica en software, para identificación, firma y cifrado	X	X	X	X					
Certificado de colectivo de médico empleado público (persona física) para identificación	X								
Certificado de colectivo de médico empleado público (persona física) para firma		X							
Certificado de cifrado en tarjeta, para médico empleado público			X	X					

6.2 Protección de la clave privada

Clave privada de la EC-OMC

La clave privada de firma de la AC es mantenida y usada en un dispositivo criptográfico seguro que cumple los requerimientos **FIPS 140-2 nivel 3**.

Para la gestión de las claves de las Autoridades de Certificación se utiliza un equipo criptográfico **homologado FIPS 140-2 nivel 3.**

Para las claves de las autoridades de OCSP y TSA se utiliza un equipo **HSM certificado FIPS 140-1 nivel 3 o custodia de claves en dispositivo smartcard con certificación CWA14169.**

Cuando al clave privada de la AC está fuera del dispositivo esta se mantiene cifrada y partida en diferentes dispositivos.

Existe un back up de la clave privada de firma de la AC, que es almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro.
Las copias de back up de la clave privada de firma de la AC están almacenadas de forma segura. Este procedimiento se describe en detalle en las políticas de seguridad de Camerfirma.

Clave privada del suscriptor
La clave privada del suscriptor se puede almacenar en un dispositivo software o hardware.
Cuando se almacene en formato software la EC OMC ofrecerá las instrucciones de configuración adecuada para un uso seguro en las aplicaciones reconocidas.
Respecto a los dispositivos criptográficos con certificados para firma electrónica avanzada, aptas como dispositivos seguros de creación de firma, cumplen el nivel de seguridad CC EAL4+ y soportan los estándares PKCS#11 y CSP.
La EC OMC utiliza como soporte criptográfico aquellos permitidos en su aplicativo de registro y que asegurarán la generación de firma electrónica reconocida:
La información respecto al tipo de creación y custodia de claves está incorporada en el propio certificado digital permitiendo a la Tercero que confía actuar en consecuencia.

6.2.1 Estándares de módulos criptográficos

Para los módulos que gestionan claves de la Entidad de Certificación de la OMC y de los suscriptores de certificados de firma electrónica, se asegurar el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2 Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de **2 de 4** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3 Depósito de la clave privada

La EC OMC no almacena ni copia claves privadas de los suscriptores cuando estas son generadas por el PSC y están sujetas a la ley 59/2003, del 19 de diciembre, de firma electrónica. Para certificados en soporte hardware es el usuario quien genera y custodia la clave privada en la tarjeta criptográfica entregada por el PSC.
La EC OMC únicamente almacenará una copia de la clave privada del suscriptor cuando esta se use "exclusivamente" para cifrado de datos o aquellos certificados asociados a las claves que no estén sujetas a la ley 59/2003, del 19 de diciembre, de firma electrónica.

6.2.4 Copia de respaldo de la clave privada

La EC OMC a través de AC Camerfirma realiza una copia de back up de las claves privadas que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de esta necesitan al menos de la participación de dos personas.
Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.
Las claves del suscriptor en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación tal como se indica en el manual de instalación de claves en software.
Las claves del suscriptor en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

6.2.5 Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenaran en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.
El suscriptor podrá almacenar las claves entregadas en software durante el periodo de duración del certificado, posteriormente deberá destruirlas asegurándose antes de que no tiene ninguna información cifrada con la clave pública.
Solo en caso de certificados de cifrado el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso la EC OMC también guardará copia de la clave privada asociada al certificado de cifrado.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de la Entidad de Certificación de la OMC, en las tarjetas colegiales o en los sistemas informáticos de los suscriptores.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de la Entidad de Certificación de la OMC.

6.2.8 Método de activación de la clave privada

La clave privada de la Entidad de Certificación de la OMC se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n.
La activación de las claves privadas de la AC Intermedia es gestionada por el aplicativo de gestión.

La clave privada del suscriptor se activa mediante la introducción del PIN en la tarjeta colegial o sistema informático.

6.2.9 Método de desactivación de la clave privada

Cuando la tarjeta colegial se retira del dispositivo lector, o cuando la aplicación que la utiliza finaliza la sesión, la clave privada se desactiva y resulta necesario nuevamente la introducción del PIN para activarla de nuevo.

Para la desactivación de la clave privada de la EC-OMC se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente, en Camerfirma.

6.2.10 Método de destrucción de la clave privada

Anteriormente a la destrucción de las claves se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.
Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de la EC-OMC. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.
Finalmente se destruirán de forma segura las copias de seguridad.
Las claves del suscriptor en software se podrán destruir mediante el borrado de estas siguiendo las instrucciones de la aplicación que las alberga.
Las claves del suscriptor en hardware podrán ser destruidas mediante un software especial en los puntos de Registro o en la EC-OMC.

6.2.11 Clasificación de módulos criptográficos

Véase la sección 6.2.1.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La Entidad de Certificación de la OMC archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de esta política.

6.3.2 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de la Entidad de Certificación de la OMC son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves. La creación y distribución de dichos dispositivos se registra.

La Entidad de Certificación de la OMC genera de forma segura los datos de activación de las tarjetas colegiales.

6.4.2 Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de la Entidad de Certificación de la OMC son protegidos por los poseedores de los mismos, que firman un contrato reconociendo sus obligaciones.

Los datos de activación de la tarjeta colegial son distribuidos separadamente de la propia tarjeta (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes, o vinculando ambos justo antes del procedimiento de entrega).

El suscriptor del certificado en software es el responsable de la protección de su clave privada, con una contraseña lo más completa posible, formada por números y letras. El suscriptor debe recordar dicha contraseña.

6.4.3 Otros aspectos de los datos de activación

Sin estipulación.

6.5 Controles de seguridad informática

La EC OMC emplea sistemas fiables para ofrecer sus servicios de certificación. La EC OMC ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, el proveedor AC Camerfirma sigue el esquema de certificación sobre sistemas de gestión de la información ISO 270001.
Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de la EC OMC, en los siguientes aspectos:

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento correcto del sistema.
4. Configuración de Usuarios y permisos.
5. Configuración de eventos de Log.
6. Plan de backup y recuperación.
7. Configuración antivirus
8. Requerimientos de trafico de red

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor de la EC OMC provisto por AC CAmerfirma incluye las siguientes funcionalidades:

- control de acceso a los servicios de la SubCA y gestión de privilegios
- imposición de separación de tareas para la gestión de privilegios
- identificación y autenticación de roles asociados a identidades
- archivo del historial del suscriptor y la SubCA y datos de auditoria
- auditoria de eventos relativos a la seguridad
- auto-diagnóstico de seguridad relacionado con los servicios de la SubCA
- Mecanismos de recuperación de claves y del sistema de la SubCA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Entidad de Certificación de la OMC son fiables, y han sido certificadas con nivel EAL 4, de acuerdo con un objetivo de seguridad específico, definido conforme a la norma ISO 15408-3:1999.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por la Entidad de Certificación de la OMC de acuerdo con estándares de desarrollo y control de cambios.
Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2 Controles de gestión de seguridad

La EC OMC desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad.
Para realizar esta función dispone de un plan de formación anual.
La EC OMC exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.1 Clasificación y gestión de información y bienes

La EC OMC mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.
La política de seguridad de la EC OMC detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.
Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.6.2.2 Operaciones de gestión

La EC OMC dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.
En el documento de seguridad de la EC OMC se desarrolla en detalle el proceso de gestión de incidencias.
La EC OMC tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema

El departamento de Sistemas de la EC OMC mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

La EC OMC dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

La EC OMC define actividades, asignadas a personas con un rol de confianza, distintas a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.3 Gestión del sistema de acceso

La EC OMC realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

AC General

Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.

Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.

La EC OMC dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

La EC OMC dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.

Cada persona tiene asociado un rol para realizar las operaciones de certificación.

El personal de la EC OMC es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la EC OMC.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de la EC OMC.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.4 Gestión del ciclo de vida del hardware criptográfico

La EC OMC a través de AC Camerfirma se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

AC Camerfirma registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

AC Camerfirma realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de la EC OMC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de la EC-OMC así como sus modificaciones y actualizaciones son documentadas y controladas.

AC Camerfirma posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.6.3 Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación.

6.7 Controles de seguridad de red

La EC OMC a través de AC Camerfirma protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.
La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

6.8 Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección 6.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de la EC-OMC subcontratadas a Camerfirma son realizadas en módulos validados al menos por **FIPS 140-1 nivel 3**.

6.9 Fuentes de Tiempo

La Autoridad de Certificación Camerfirma que provee la infraestructura para la prestación de los servicios de certificación a EC OMC tiene un procedimiento de sincronización de tiempo coordinado con el ROA Real Instituto y Observatorio de la Armada en San Fernando vía NTP También obtiene una fuente segura vía GPS y sincronización vía Radio.

7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

La Entidad de Certificación de la OMC publica sus perfiles de certificados en el Depósito.

Todos los certificados cualificados o reconocidos emitidos bajo esta política están en conformidad con el estándar X.509 versión 3 y al RFC 3739 y ETSI 101 867 “Qualified Certificate Profile”.

7.1.1 Número de versión

La EC OMC emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Los documentos de las extensiones de los certificados se encuentran detallados en documentos independientes que pueden ser accedidos desde la página Web de la EC OMC.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.5 sha1WithRSAEncryption
- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos

Adicionalmente se pueden establecer restricciones de nombres en relación con los certificados a la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica, siempre que las mismas resulten objetivas, proporcionadas, transparentes y no discriminatorias.

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

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos partiendo de la siguiente raíz 1.3.6.1.4.1.26852.

Certificado	OID
Certificado corporativo de colegiado (persona física) para identificación	1.3.6.1.4.1.26852.1.1.1.1
Certificado corporativo de colegiado (persona física) para firma	1.3.6.1.4.1.26852.1.1.1.2
Certificado corporativo de colegiado (persona física) para cifrado	1.3.6.1.4.1.26852.1.1.1.3
Certificado corporativo de colegiado (persona física), en SOFTWARE, para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.7
Certificado corporativo de colegiado (persona física), en HSM, para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.9
Certificado corporativo de personal administrativo (persona física) para identificación	1.3.6.1.4.1.26852.1.1.2.1
Certificado corporativo de personal administrativo (persona física) para firma	1.3.6.1.4.1.26852.1.1.2.2
Certificado de cifrado en tarjeta, para personal administrativo	1.3.6.1.4.1.26852.1.1.2.3
Certificado corporativo de personal administrativo (persona física), en software, para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.6

Certificado corporativo de persona jurídica para identificación	1.3.6.1.4.1.26852.1.1.3.1
Certificado corporativo de persona jurídica para firma	1.3.6.1.4.1.26852.1.1.3.2
Certificado de cifrado en tarjeta, para persona jurídica	1.3.6.1.4.1.26852.1.1.3.3
Certificado corporativo de persona jurídica en software, para identificación, firma y cifrado	1.3.6.1.4.1.26852.1.1.5
Certificado de colectivo de médico empleado público (persona física) para identificación	1.3.6.1.4.1.26852.1.2.1.1
Certificado de colectivo de médico empleado público (persona física) para firma	1.3.6.1.4.1.26852.1.2.1.2
Certificado de cifrado en tarjeta, para médico empleado público	1.3.6.1.4.1.26852.1.2.1.3

7.2 Perfil de la lista de revocación de certificados

La Entidad de Certificación de la OMC publica sus perfiles de listas de revocación.

7.2.1 Número de versión

Las CRL emitidas por la EC OMC son de la versión 2.

7.2.2 Perfil de OCSP

Según el estándar IETF RFC 2560.

8 Auditoria de conformidad

La EC OMC es una empresa comprometida con la seguridad y la calidad de sus servicios por ello confía en el proveedor AC Camerfirma para la prestación de los servicios de certificación.

Los objetivos de AC Camerfirma respecto a la seguridad y la calidad del servicio son demostrados mediante la obtención y mantenimiento de la certificación **ISO/IEC 27001:2005**, **ISO/IEC 20000-1:2007**, la realización de Auditorías internas bienales al sistema de la autoridad de certificación, y fundamentalmente a las Autoridades de registro, para garantizar el cumplimiento de los procedimientos internos.

AC Camerfirma está sujeta a unas auditorias periódicas respecto a los principios y criterios de los sellos **WEBTRUST for CA, WEBRUST SSL BR Requirements y WEBTRUST EV** que asegura que los documentos de políticas y CPS tienen un formato y alcance adecuado a la vez que están completamente alineadas con su políticas y prácticas de certificación.

AC Camerfirma pasó con éxito en el año **2007** un proceso de inspección ordinaria del Ministerio de Industria. El Ministerio de Industria es el ente regulador encargado de supervisar las actividades llevadas a cabo por los prestadores de servicios de certificación españoles.

Del mismo modo, EC OMC se encuentra registrada como prestador de servicios de certificación aprobado por el Ministerio de Industria y sometido a las revisiones de control que este organismo considere necesarias.

Las Autoridades de Registros pertenecientes a esta jerarquía están sujetas a un proceso de auditoría interna. Estas auditorías se realizan periódicamente con una frecuencia no superior a 2 años. La frecuencia de las auditorias (1 o 2 años) a las autoridades de registro son calculadas por el número de certificados emitidos y número de operadores de registro.

8.1 Frecuencia de la auditoria de conformidad

AC Camerfirma lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad. La EC OMC al incorporarse en la jerarquía de AC Camerfirma para la prestación de los servicios de certificación, se encuentra sometida a los controles requeridos por la AC Camerfirma de manera adicional a los propios controles internos de cumplimiento y adecuación de los servicios ofrecidos.

8.2 Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados, de acuerdo con las especificaciones técnicas ETSI TS 101 456 y TS 102 042

8.3 Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la AC.

8.4 Listado de elementos objeto de auditoria

La auditoría verifica respecto a la Autoridad de Certificación de Camerfirma y por ende a la EC OMC que se integra en esta:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la Política de Certificación, DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de AC Camerfirma, ARs y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento llevada a cabo, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si la Entidad de Certificación auditada es incapaz de desarrollar y / o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá comunicar inmediatamente al Consejo General de Colegios Oficiales de Médicos de España y AC Camerfirma, que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Entidad de Certificación, y regenerar la infraestructura.
- Terminar el servicio de la Entidad de Certificación
- Otras acciones complementarias que resulten necesarias.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Consejo General de Colegios Oficiales de Médicos de España en un plazo máximo de 15 días tras la ejecución de la auditoría.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

La Entidad de Certificación de la OMC ha establecido una tarifa por la emisión o por la renovación de los certificados, que se suministra oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a certificados

La Entidad de Certificación de la OMC no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

La Entidad de Certificación de la OMC no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación.

9.1.5 Política de reintegro

Los suscriptores tienen derecho al desistimiento del contrato en el plazo máximo de siete días desde la recepción del mismo, sin que el ejercicio de dicho derecho pueda ocasionar penalización alguna.

9.2 Capacidad financiera

La Entidad de Certificación de la OMC dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios.

9.2.1 Cobertura de seguro

La Entidad de Certificación de la OMC dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional por errores y omisiones, con un mínimo asegurado de 3.000.000 de euros.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados

La Entidad de Certificación de la OMC dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional por errores y omisiones, con un mínimo asegurado de 3.000.000 de euros.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por la Entidad de Certificación de la OMC:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

9.3.2 Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos del poseedor de claves, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico del poseedor de claves, o la dirección de correo electrónico asignada por el suscriptor.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Toda otra información que no esté indicada en la sección anterior.

9.3.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

La Entidad de Certificación de la OMC divulga la información confidencial en los casos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado son divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

La Entidad de Certificación indicará estas circunstancias en la política de intimidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

La Entidad de Certificación de la OMC incluye, en la política de intimidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del poseedor de claves, directamente a los mismos o a terceros.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de datos personales

Para la prestación del servicio, la Entidad de Certificación de la OMC precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones son recabadas principalmente a través de los suscriptores, en base a la relación corporativa que les une con los poseedores de claves (colegiados, órganos colegiales, personal administrativo o custodios de certificados de persona jurídica) o directamente de los afectados, bien con su consentimiento explícito o sin el mismo, en los casos en los que la ley permita recabar la información sin consentimiento del afectado.

La Entidad de Certificación recaba los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.

La Entidad de Certificación ha desarrollado una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documentado en su Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de trece de diciembre de 1999, de protección de datos de carácter personal. Esta Declaración de Prácticas de Certificación tiene, por tanto, la consideración de documento de seguridad.

La Entidad de Certificación no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8, en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en este documento, que cumplen las obligaciones previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de trece de diciembre de 1999, de protección de datos de carácter personal.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

La Entidad de Certificación de la OMC es la única entidad que goza de los derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de lo derechos de los suscriptores, poseedores de claves y terceros, concediendo licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con las correspondientes condiciones generales de emisión/uso.

Adicionalmente, los certificados emitidos por la Entidad de Certificación contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2 Propiedad de la Declaración de Prácticas de Certificación

La Entidad de Certificación de la OMC es la única entidad que goza de los derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, el poseedor de claves, conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de la Entidad de Certificación de la OMC

La Entidad de Certificación de la OMC garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política de certificado para la que emite certificados, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso cuando una parte o la totalidad de las operaciones se subcontratan externamente.

La Entidad de Certificación prestar los servicios de certificación conforme con esta Declaración de Prácticas de Certificación.

Antes de la emisión y entrega del certificado al suscriptor, la Entidad de Certificación le informa de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso.

Este requisito se cumple mediante un “Texto divulgativo de la política de certificado” aplicable, que puede ser transmitido electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

La Entidad de Certificación vincular a suscriptores, poseedores de claves y terceros que confían en certificados mediante condiciones generales de la contratación, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.2, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.

- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público y de la necesidad de empleo de la tarjeta como dispositivo seguro de creación de firma o descifrado de mensajes.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión de la tarjeta colegial/dispositivo seguro de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

La Entidad de Certificación de la OMC, en las condiciones generales que la vinculan con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La Entidad de Certificación, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.

- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

La Entidad de Certificación, como mínimo, garantizará al tercero que confía en el certificado:
- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, la Entidad de Certificación garantiza al suscriptor y al tercero que confía en el certificado:
- Que el certificado contiene las informaciones que debe contener un certificado reconocido, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, poseedor de claves, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.3 Rechazo de otras garantías

La Entidad de Certificación de la OMC rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4 Limitación de responsabilidades

La Entidad de Certificación limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores y tarjetas colegiales con la consideración de dispositivo

seguro (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por la Entidad de Certificación.

9.6.5 Cláusulas de indemnidad

9.6.5.1 Cláusula de indemnidad de suscriptor

La Entidad de Certificación de la OMC incluye, en las condiciones generales de emisión, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2 Cláusula de indemnidad de tercero que confía en el certificado

La Entidad de Certificación de la OMC incluye, en las condiciones generales de uso, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6 Caso fortuito y fuerza mayor

La Entidad de Certificación de la OMC incluye cláusulas en las condiciones generales de emisión/uso para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7 Ley aplicable

La Entidad de Certificación establece, en las condiciones generales de emisión/uso, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

9.6.8 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

La Entidad de Certificación de la OMC establece, en las condiciones generales de emisión/uso, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9 Cláusula de jurisdicción competente

La Entidad de Certificación de la OMC establece, en las condiciones generales de uso/emisión, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10 Resolución de conflictos

La Entidad de Certificación de la OMC establece, en las condiciones generales de emisión/uso, los procedimientos de mediación y resolución de conflictos aplicables.