Servicio de Certificación Digital

Organización Médica Colegial de España

Declaración de Prácticas de Certificación
Autoridad 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
3.1	En todo el documento	• Modificaciones sugeridas por el supervisor nacional	ASTREA	14/12/2016

		• Inclusión de nuevos certificados	ASTREA	20/03/2017
		○ Se añade información de los perfiles de órgano colegial. ○ Se añade información del perfil de representante de PJ en software.	ASTREA	15/06/2017
		○ Adaptación de las modificaciones por REIDAS en la CPS de Camerfirma	ASTREA	28/06/2017
		○ Revisión punto 1.3.4.2 de Jerarquía de Certificación, tras las indicaciones del Supervisor	ASTREA	03/05/2018
		○ Revisión tras las indicaciones de la Auditoría de seguimiento	ASTREA	17/12/2018
		○ Cambio responsable aprobación de la documentación	ASTREA	30/01/2019
3.2	5.3.2 y 9.4	○ Actualización legislación	ASTREA	29/03/2019
3.3	6.1	○ Indicación del tiempo de validez de los certificados de entidad final	ASTREA	12/07/2019
	1.1; 1.2; 1.3	○ Eliminación del certificado externo de médico empleado público	ASTREA	25/07/2019
	1.3; 1.4; 3.1; 3.2; 3.5; 4.1; 4.4; 4.7; 4.9	○ Eliminación referencias a los Servicios Autonómicos de Salud por eliminación del certificado externo de médico empleado público	ASTREA	25/07/2019
	1.5.3	○ Se añade intervalo máximo de revisión de la configuración del sistema.	ASTREA	29/07/2019
	5.3.7; 5.3.8	○ Se arreglan errores de formato	ASTREA	29/07/2019

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 cualificados 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 Autoridad 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 Autoridad de Certificación de la Organización Médica Colegial.

Los certificados que se emiten son los siguientes:

- Certificados **corporativos** de:
  - Médico/a colegiado/a
  - Personal administrativo
  - Órgano Colegial
  - Sello electrónico de persona jurídica
  - Representante legal de persona jurídica

Los servicios de certificación prestados por la Autoridad 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 Autoridad 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 Autoridad de Certificación de la OMC.

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	Soporte	Usos	OID
De Médico Colegiado	Tarjeta	Autenticación	1.3.6.1.4.1.26852.1.1.1.1
		Firma	1.3.6.1.4.1.26852.1.1.1.2
		Cifrado	1.3.6.1.4.1.26852.1.1.1.3

	Software	Autenticación, Firma y Cifrado	1.3.6.1.4.1.26852.1.1.7
De Personal Administrativo	Tarjeta	Autenticación	1.3.6.1.4.1.26852.1.1.2.1
		Firma	1.3.6.1.4.1.26852.1.1.2.2
		Cifrado	1.3.6.1.4.1.26852.1.1.2.3
	Software	Autenticación, Firma y Cifrado	1.3.6.1.4.1.26852.1.1.6
De Organo Colegial	Tarjeta	Autenticación	1.3.6.1.4.1.26852.1.1.4.1
		Firma	1.3.6.1.4.1.26852.1.1.4.2
		Cifrado	1.3.6.1.4.1.26852.1.1.4.3
	Software	Autenticación, Firma y Cifrado	1.3.6.1.4.1.26852.1.1.8
De Representante Legal	Tarjeta	Autenticación	1.3.6.1.4.1.26852.1.1.11.1
		Firma	1.3.6.1.4.1.26852.1.1.11.2
		Cifrado	1.3.6.1.4.1.26852.1.1.11.3
	Software	Autenticación, Firma y Cifrado	1.3.6.1.4.1.26852.1.1.12
De Sello electrónico de Persona Jurídica	DCCF	Autenticación, Firma y Cifrado	1.3.6.1.4.1.26852.1.1.10.1
	Software	Autenticación, Firma y Cifrado	1.3.6.1.4.1.26852.1.1.10.2

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
Certificados de persona jurídica en tarjeta (I)	1.3.6.1.4.1.26852.1.1.3.1	Identificación
Certificados de persona jurídica en tarjeta (F)	1.3.6.1.4.1.26852.1.1.3.2	Firma
Certificados de persona jurídica en tarjeta (I)	1.3.6.1.4.1.26852.1.1.3.3	Cifrado
Certificados de persona jurídica en software	1.3.6.1.4.1.26852.1.1.5	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 cualificados, 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.

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 Autoridad 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.

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.

Por su parte, 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 los usos de firma electrónica, autenticación y cifrado.

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

1) Solicitantes de certificados.
2) Suscriptores del servicio de certificación.
3) Firmantes y personas responsables de los datos de creación de sellos electrónicos .
4) Partes usuarias.

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) Otras personas jurídicas del ámbito sanitario que dispongan de convenio con la OMC.

1.3.3.2 Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son las entidades que los adquieren a la Autoridad de Certificación para su uso en su ámbito corporativo, incluyendo los colegios profesionales, otras personas jurídicas del ámbito sanitario.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, al objeto de facilitar el acceso al certificado a una persona concreta, debidamente autorizada, y que figura identificada en el certificado, como se indica en el siguiente epígrafe.

El suscriptor del servicio de certificación es, por tanto, el cliente de la Autoridad de Certificación, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por la Autoridad de Certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes y las personas responsables de los datos de creación de los sellos electrónicos de persona jurídica, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados, en especial ETSI EN 319 411-2, secciones 5.4.2 y 6.3.4.e)

1.3.3.3 Firmantes y creadores de sellos

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma digital (para identificación y firma electrónica cualificada) y de descifrado del certificado; esto es, típicamente los colegiados/as, los órganos colegiales, los representantes legales, el personal administrativo de los colegios y otras organizaciones.

Los creadores de sellos son aquellas personas responsables de los datos de creación de los sellos electrónicos de persona jurídica.

Los firmantes y personas responsables de los datos de creación de sellos electrónicos de persona jurídica se encuentran debidamente autorizados 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 las personas físicas identificadas en los correspondientes certificados 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.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la identificación o el cifrado, donde podría resultar confuso el empleo de los términos firmante o persona responsable de los datos de creación de sellos electrónicos de persona jurídica, se emplea el término más genérico de “persona física identificada en el certificado”, siempre con pleno respeto al cumplimiento de la legislación de firma electrónica en relación con los derechos y obligaciones del firmante y de la persona responsable de los datos de creación de sellos electrónicos de persona jurídica.

1.3.3.4 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones de la Autoridad de Certificación.

1.3.4 Otros participantes

1.3.4.1 Proveedores técnicos

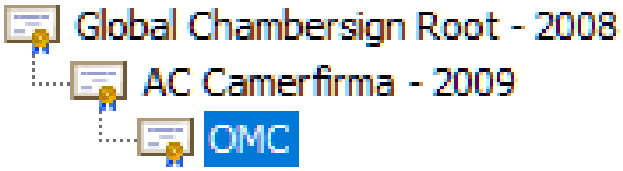
La Autoridad de Certificación de la OMC se apoya en los servicios de certificación que ofrece el proveedor técnico CAMERFIRMA.

Asimismo, la Autoridad de Certificación de la 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.

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



1.3.4.2.1 AC-OMC – Autoridad de certificación subordinada

Es la Autoridad 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 “AC Camerfirma – 2009”

En este caso, CAMERFIRMA actuará como prestador de servicios de certificación subcontratado para la Autoridad de Certificación de la Organización Médica Colegial (AC-OMC).

La AC-OMC tiene la siguiente descripción técnica:

Certificate serial: 484251359877222014
Issuer: CN=AC Camerfirma - 2009, L=Madrid (see current address at https://www.camerfirma.com/address), SERIALNUMBER=A82743287, O=AC Camerfirma S.A., C=ES
Subject: CN=OMC, OU=ENTIDAD DE CERTIFICACION, O=ORGANIZACION MEDICA COLEGIAL, C=ES
Validity: 2014-11-24 12:07:55 - 2024-11-21 12:07:55
Huella digital SHA1: A2:18:EF:ED:DE:AB:DC:0B:30:DB:08:F6:93:B7:8A:46:A6:8A:FC:9B
Huella digital SHA256: C1:76:11:DB:7B:31:13:61:E2:0D:7B:82:31:AA:DF:47:8B:CB:7F:FA:0B:E5:85:C0:6D:E2:30:92:23:C2:EF:8A

El OID de la AC-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 Certificados corporativos de colegiado/a en tarjeta

1.4.1.1.1 Aspectos comunes

Los certificados corporativos de colegiado son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados corporativos de colegiado funcionan con dispositivo cualificado de creación de firma electrónica, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

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 firmante y, en consecuencia, es el poseedor 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.

1.4.1.1.2 Certificado corporativo de colegiado/a para identificación

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.1.1
OID política NCP+	0.4.0.2042.1.2

Los certificados corporativos de colegiado (de identificación) garantizan la identidad de la persona poseedora de la clave privada de identificación, y su vinculación con el suscriptor del servicio de certificación.

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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación” del médico colegiado/a”.

1.4.1.1.3 Certificado corporativo de colegiado/a para firma

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.1.2
OID política QCP-n-qscd	0.4.0.194112.1.2

Los certificados corporativos de colegiado (de firma) permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual, de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" nos describe que el uso de este certificado es para la "firma electrónica cualificada de médico colegiado/a".

1.4.1.1.4 Certificado de cifrado para colegiado, en tarjeta

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.1.3

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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 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) 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 cualificado.
c) QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
d) El campo “User Notice” nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.2 <u>Certificados corporativos de colegiado en software</u>

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.7
OID política QCP-n	0.4.0.194112.1.0

Los certificados corporativos de colegiado en software de firma electrónica avanzada son certificados cualificados de acuerdo con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados corporativos de colegiado en software software no garantizan su funcionamiento con dispositivos seguros de creación de firma electrónica, a los que se refiere el anexo II del Reglamento (UE) 910/2014.

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

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Por otra parte, los certificados corporativos de colegiado 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 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:

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

En todo caso, se deberá utilizar la clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y a la persona indicada en el certificado 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
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 cualificado.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación, firma electrónica avanzada y el cifrado del médico colegiado, en software”.

1.4.1.3 Certificados corporativos de personal administrativo en tarjeta

1.4.1.3.1 Aspectos comunes

Los certificados corporativos de personal administrativo son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados corporativos de personal administrativo funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014..

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

1.4.1.3.2 Certificado corporativo de personal administrativo para identificación

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.2.1

OID política QCP-n-qscd	0.4.0.194112.1.2

Los certificados corporativos de personal administrativo (de identificación) garantizan la identidad de la persona poseedora de la clave privada de identificación, y su vinculación con el suscriptor del servicio de certificación.

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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación de personal administrativo y de servicios”.

1.4.1.3.3 Certificado corporativo de personal administrativo para firma

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.2.2
OID política QCP-n-qscd	0.4.0.194112.1.2

Los certificados corporativos de personal administrativo (de firma) permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual, de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

Asimismo, incluyen una manifestación relativa a la categoría del firmante, que ha sido comprobada antes de emitir el certificado, y es correcta. Es necesario advertir que esta

indicación no es, por si sola, suficiente por determinar las facultades que tiene el firmante para firmar, en su caso, en nombre del suscriptor del servicio de certificación; por lo tanto, la parte usuaria tendrá que comprobar las facultades y poderes de firma del firmante mediante otros medios, diferentes al certificado, como por ejemplo el servicio de validación de la OMC.

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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica cualificada de personal administrativo y de servicios”.

1.4.1.3.4 Certificado de cifrado de personal administrativo, en tarjeta

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.2.3

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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 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) 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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.4 Certificados corporativos de personal administrativo en software

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.6
OID política QCP-n	0.4.0.194112.1.0

Los certificados corporativos de personal administrativo en software de firma electrónica avanzada son certificados cualificados de acuerdo con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados corporativos de personal administrativo en software no garantizan su funcionamiento con dispositivos seguros de creación de firma electrónica, a los que se refiere el anexo II del Reglamento (UE) 910/2014.

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

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Por otra parte, los certificados corporativos de personal administrativo 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 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 de la persona indicada en el certificado.
d) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de ls persona indicada en el certificado.

En todo caso, se deberá utilizar la clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y a la persona indicada en el certificado 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
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 cualificado.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica avanzada y cifrado del personal administrativo en software”.

1.4.1.5 Sellos electrónicos de persona jurídica

1.4.1.5.1 Aspectos comunes

Los certificados de sello electrónico de persona jurídica son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados garantizan la identidad del subscriptor, es decir del Colegio de Médicos u cualquier otra persona jurídica del ámbito sanitario público o privado y, en su caso, de la persona que lo gestiona, incluidos en el certificado.

1.4.1.5.2 Certificado de sello electrónico de persona jurídica en DCCF

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.10.1
OID política QCP-n-qscd	0.4.0.194112.1.3

Estos certificados funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

La AC-OMC no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Content commintment (para realizar la función de firma electrónica)
   - Key Encipherment (para gestión y tansporte de claves)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:

- QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
- QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" nos describe el uso de este certificado.

1.4.1.5.3 Certificado sello electrónico de persona jurídica en software

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.10.2
OID política QCP-n	0.4.0.194112.1.1

La AC-OMC no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

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

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Content commintment (para realizar la función de firma electrónica)
   - Key Encipherment (para gestión y tansporte de claves)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo "User Notice" nos describe el uso de este certificado.

1.4.1.6 Certificados corporativo de Representante de Persona Jurídica en tarjeta

1.4.1.6.1 Aspectos comunes

Los certificados corporativos de Representante de PJ son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados corporativos de Representante de PJ funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento general entre el firmante y una entidad, colegio de médicos u organización del ámbito sanitario, descrita en el campo "O" (Organization), y permiten la generación de la "firma electrónica cualificada" es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

1.4.1.6.2 Certificado corporativo de representante de PJ para identificación

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.11.1
OID política QCP-n-qscd	0.4.0.194112.1.2
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

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 cualificado.

b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

1.4.1.6.3 Certificado corporativo de representante de PJ, para firma

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.11.2
OID política QCP-n-qscd	0.4.0.194112.1.2
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

Los certificados corporativos de representante de PJ (de firma) permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual, de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

Asimismo, incluyen una manifestación relativa a la categoría del firmante, que ha sido comprobada antes de emitir el certificado, y es correcta. Es necesario advertir que esta indicación no es, por si sola, suficiente por determinar las facultades que tiene el firmante para firmar, en su caso, en nombre del suscriptor del servicio de certificación; por lo tanto, la parte usuaria tendrá que comprobar las facultades y poderes de firma del firmante mediante otros medios, diferentes al certificado, como por ejemplo el servicio de validación de la OMC.

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:
    - qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

1.4.1.6.4 Certificado de cifrado de representante de PJ, en tarjeta

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.11.3
OID política NCP+	0.4.0.2042.1.2
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 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) 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 cualificado.

b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

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

1.4.1.7 Certificados corporativos de Representante de Persona Jurídica, en software

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.12
OID política QCP-n	0.4.0.194112.1.0
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

Los certificados corporativos de representante de persona jurídica en software de firma electrónica avanzada son certificados cualificados de acuerdo con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados corporativos de representante de persona jurídica en software no garantizan su funcionamiento con dispositivos seguros de creación de firma electrónica, a los que se refiere el anexo II del Reglamento (UE) 910/2014.

Estos certificados se emiten a representantes de persona jurídica, en el ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".
Por otra parte, los certificados corporativos de representante 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 representante 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 de la persona indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona indicada en el certificado.

En todo caso, se deberá utilizar la clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y a la persona indicada en el certificado 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
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 cualificado.
c) El campo "User Notice" nos describe que el uso de este certificado es para la "firma electrónica avanzada y cifrado del representante legal en software".

1.4.1.8 Certificados corporativos de Órgano Colegial en tarjeta

1.4.1.8.1 Aspectos comunes

Los certificados corporativos de Órgano Colegial son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados corporativos de órgano colegial funcionan con dispositivo cualificado de creación de firma electrónica, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados se emiten a colegiados como órganos colegiales del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso. Este órgano tiene la consideración de firmante y, en consecuencia, es el poseedor de la tarjeta y el software complementario correspondientes.

Asimismo, incluyen una manifestación relativa a la categoría o el cargo orgánico del fimante, que han sido comprobados antes de emitir el certificado, y son correctos.

1.4.1.8.2 Certificado corporativo de órgano colegial para identificación

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.4.1
OID política NCP+	0.4.0.2042.1.2

Los certificados corporativos de órgano colegial (de identificación) garantizan la identidad de la persona poseedora de la clave privada de identificación, y su vinculación con el suscriptor del servicio de certificación.

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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación” del órgano colegial”.

1.4.1.8.3 Certificado corporativo de órgano colegial para firma

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.4.2
OID política QCP-n-qscd	0.4.0.194112.1.2

Los certificados corporativos de órgano colegial (de firma) permiten la generación de la “firma electrónica cualificada”; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual, de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

Por otra parte, los certificados corporativos de órgano colegial (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 cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “firma electrónica cualificada del órgano colegial”.

1.4.1.8.4 Certificado de cifrado para órgano colegial, en tarjeta

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.4.3

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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 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) 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 cualificado.

b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

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

1.4.1.9 Certificados corporativos de órgano colegial en software

OID jerarquía de la OMC	1.3.6.1.4.1.26852.1.1.8
OID política QCP-n	0.4.0.194112.1.0

Los certificados corporativos de órgano colegial en software de firma electrónica avanzada son certificados cualificados de acuerdo con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Los certificados corporativos de órgano colegial en software no garantizan su funcionamiento con dispositivos seguros de creación de firma electrónica, a los que se refiere el anexo II del Reglamento (UE) 910/2014.

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

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, los certificados corporativos de órgano colegial 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 órgano colegial 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 de la persona indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona indicada en el certificado.

En todo caso, se deberá utilizar la clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y a la persona indicada en el certificado 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
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 cualificado.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación, firma electrónica avanzada y el cifrado del órgano colegial, en software”.

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 https://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 suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, el firmante o la persona responsable de la custodia 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 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.

1.5 Administración de la política

1.5.1 Organización que administra el documento

COMISIÓN PERMANENTE DEL 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
EMAIL: CERTIFICACION@CGCOM.ES

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 Autoridad 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.

Se establece en 6 meses el intervalo máximo de revisión periódica de los sistemas de la Autoridad de Certificación de la OMC, de acuerdo con el documento “Procedimiento de configuración de sistemas”.

2 Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

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

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona física identificada en el certificado.
- 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, en lengua española e inglesa.
- Los textos de divulgación (PKI Disclosure Statements – PDS), en lengua española e inglesa.

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 Autoridad 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 Autoridad 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 la persona física identificada en el certificado 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 de la persona física identificada en el certificado, 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 (Tarjeta, Software)

Country (C)	“ES”
Organization (O)	Colegio profesional
Surname	Apellidos
Given Name	Nombre
Title	“Médico colegiado/a”
Serial Number	DNI/NIE, en formato ETSI
Common Name (CN)	Nombre, apellidos y número del DNI/NIE
DirectoyName (CGCOM.2.4)	Nombre y apellidos del colegiado

3.1.1.2 Certificado corporativo de personal administrativo (Tarjeta, Software)

Country (C)	“ES”
Organization (O)	Colegio profesional
Surname	Apellidos
Given Name	Nombre
Title	"Personal administrativo y de servicios”
Serial Number	DNI/NIE, en formato ETSI
Common Name (CN)	Nombre y apellidos y número del DNI/NIE

DirectoryName (CGCOM.2.8)	Nombre y apellidos del personal administrativo

3.1.1.3 Certificado corporativo de Representante legal (Tarjeta o Software)

Country (C)	"ES"
Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario
Surname	Apellidos
Given Name	Nombre
Serial Number	DNI/NIE del representante, en formato ETSI
Common Name (CN)	DNI Representante legal, nombre y apellidos, NIF del Colegio o PJ representada.

3.1.1.4 Certificado corporativo de Sello electrónico (DCCF o Software)

Country (C)	"ES"
Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario
Serial Number	NIF de la persona jurídica

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 representante legal y un colegio profesional español, con independencia de la nacionalidad del colegiado, empleado o representante legal. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, empleado o representante legal la persona autorizada a su uso.
El campo “número de serie” debe incluir el DNI o el NIE del colegiado, empleado o al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de la Autoridad 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, 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 Autoridad 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 las personas físicas identificadas en dichos certificados corporativos – colegiados/as, órganos colegiales, representantes de persona jurídica y personal administrativo – se valida mediante los registros corporativos de la entidad.

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.

En relación a los datos personales de cada entidad, empresa u organización de derecho público o privado, EC-OMC actúa como encargado del tratamiento en los términos indicados en al apartado 9.4 de este documento.

3.2.1 Prueba de posesión de clave privada

El par de claves es generado por la Autoridad 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 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*".

3.2.2.3 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.

3.2.2.4 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 Autoridad de Certificación de la OMC y cada una de estas entidades jurídicas del ámbito sanitario.

3.2.2.5 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 las personas físicas identificadas en los 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 Necesidad de presencia personal

En general, no se requiere presencia física directa para la solicitud 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 Autoridad de Certificación de la OMC deberá contrastar la identidad de la persona física identificada en el certificado mediante la presencia física 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 o de la Entidad jurídica del ámbito sanitario, se confirma fehacientemente la validación de la identidad de la persona física identificada en el certificado.

Por este motivo, en todos los casos en que se expide un certificado se verifica presencialmente la identidad de la persona física en cada procedimiento de expedición de un certificado.

3.2.3.3 Vinculación de la persona física con una organización

La justificación documental de la vinculación de una persona física identificada en un certificado con el Colegio o la Entidad jurídica del ámbito sanitario es la propia solicitud y su presencia en el registro de médicos del Colegio (para colegiados) o en otros registros internos (para personal administrativo u órganos colegiados).

3.2.4 Información de suscriptor no verificada

La Autoridad 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 Autoridad de Certificación de la OMC comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en un certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son los siguientes:

- El uso de una "frase de comprobación de identidad", que consiste en información que sólo conoce la persona física identificada en el certfiicado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación, siempre que se trate de un certificado expedido por la AC-OMC y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona física identificada en el certificado 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 Autoridad de Certificación de la OMC comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos, en cuyo caso se aplicará lo dispuesto en la sección anterior

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 física identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona fisica identificada en el certificado 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 Autoridad 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 o de la persona física identificada en el certificado, firmada electrónicamente.
- El uso de la "frase de comprobación de identidad", que consiste en información que sólo conoce la persona física identificada en el certificado, y que le permite revocar de forma automática su certificado.
- La personación física en una oficina de un Colegio de Médicos.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de la Autoridad 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 Autoridad de Certificación de la OMC (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 o CGCOM 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 o una Entidad del ámbito santiario.

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 Autoridad 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 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 a la Autoridad 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 de la persona física identificada en el certificado, de acuerdo con lo establecido

en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

Asimismo, el Colegio o la Entidad del ámbito sanitario 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad de Certificación o de los suscriptores, la Autoridad 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 Autoridad de Certificación notifica al solicitante la aprobación o denegación de la solicitud.

4.2.3 Plazo para resolver la solicitud

La Autoridad 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 Autoridad 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 a la persona física identificada en el certificado 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 Autoridad 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 de la persona física identificada en el certificado.
- 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 Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, 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.

4.3.2 Notificación de la emisión al suscriptor

La Autoridad de Certificación de la OMC notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades de la Autoridad de Certificación de la OMC

La Autoridad de Certificación:

- Acredita definitivamente la identidad de la persona física identificada en el certificado, con la colaboración del Colegio o la Entidad del ámbito sanitario suscriptor, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Entrega a la persona física identificada en el certificado. con la colaboración del Colegio o la Entidad del ámbito sanitario suscriptor, cuando sea necesario, la tarjeta que contiene el certificado.
- Entrega a la persona física identificada en el certificado, con la colaboración del Colegio o la Entidad del ámbito sanitario 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 de la persona física identificada en el certificado.
e) Responsabilidad de la persona física identificada en el certificado.
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 Autoridad de Certificación de la OMC. Para ello, la Autoridad 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 persona física identificada en el certificado. sus datos de activación de firma y otras informaciones.

Las tarjetas se entregan protegidas, de forma que únicamente la persona física identificada en el certificado puede hacer uso de las mismas.

4.4.2 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación ante el Colegio o la Entidad jurídica del ámbito sanitario suscriptor.

Cuando la persona física identificada en el certificado 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 Autoridad 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, siempre que se disponga de la autorización de la persona física identificada en el certificado.

4.4.4 Notificación de la emisión a terceros

La Autoridad 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 firmante

La Autoridad de Certificación de la OMC obliga al firmante a:

- Facilitar a la AC-OMC 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 **Error! Reference source not found.**.
- Cuando el certificado funcione conjuntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas cualificadas; 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 **Error! Reference source not found.**, **Error! Reference source not found.** y **Error! Reference source not found.**.
- Comunicar a la AC-OMC y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - 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.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

- Dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación o de compromiso de las claves de la CA.

4.5.2 Responsabilidad civil del firmante

La AC-OMC obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante 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 certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante 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 título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3 Uso por el suscriptor

4.5.3.1 Obligaciones del suscriptor del certificado

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

- Facilitar a la Autoridad 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.
- Comunicar a la Autoridad de Certificación y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  a) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

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

- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Autoridad 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 Autoridad de Certificación de la OMC, sin permiso previo por escrito.

4.5.3.2 Responsabilidad civil del suscriptor de certificado

La Autoridad 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.

4.5.4 Uso por el tercero que confía en certificados

4.5.4.1 Obligaciones del tercero que confía en certificados

La Autoridad 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 cualificadas; 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 Autoridad de Certificación de la OMC, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Autoridad de Certificación de la OMC, sin permiso previo por escrito.

4.5.4.2 Responsabilidad civil del tercero que confía en certificados

La Autoridad 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 la entidad jurídica del ámbito sanitario.

4.7.3 Procedimientos de solicitud de renovación

4.7.3.1 Realización de la solicitud

La Autoridad 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 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 o la Entidad jurídica del ámbito sanitario a la Autoridad 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 a la persona física identificada en el certificado..

Asimismo, el Colegio o la Entidad jurídica del ámbito sanitario 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 Autoridad de Certificación debe aprobar la solicitud de renovación del certificado y proceder a su emisión y entrega.

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

4.7.3.4 Plazo para resolver la solicitud

La Autoridad 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 Autoridad de Certificación de la OMC notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.7.5 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación ante el suscriptor.

Cuando la persona física identificada en el certificado 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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 la persona física identificada en el certificado, 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 de la persona física identificada en el certificado.

4) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado.:

a) Finalización de la relación jurídica de prestación de servicios entre la Autoridad 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 a la persona física identificada en el certificado..

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

d) Infracción por el suscriptor o por la persona física identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento de la persona física identificada en el certificado.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor a la persona física identificada en el certificado. o la finalización de la relación entre suscriptor y persona física identificada en el certificado..

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 de la persona física identificada en el certificado a las quejas recibidas.

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La propia persona identificada en el certificado.
- Un representante autorizado por el suscriptor.
- La Autoridad 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 Autoridad de Certificación de la OMC o, en su caso, al Colegio, o el registrador que tramitó la solicitud de certificación, comprensiva de la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor y del firmante.
- 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.

La AC-OMC podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación[1].

El servicio de revocación se encuentra en la página de la Web de la AC 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 una persona física identificada en el certificado. fuera el Colegio o la Entidad jurídica del ámbito sanitario suscriptor, una vez autenticada la solicitud debe remitir una solicitud en este sentido a la Autoridad de Certificación de la OMC.

[1] Ap 6.2.4.a) iii) de ETSI EN 319 411-1

La solicitud de revocación será procesada a su recepción.

Se informa al suscriptor y, en todo caso, a la persona física identificada en el certificado., acerca del cambio de estado del certificado revocado.

La Autoridad 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 AC 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, y no será superior a las 24 horas[2].

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 Autoridad 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 Autoridad 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 Autoridad de Certificación de la OMC, así como en las siguientes direcciones web, indicadas dentro de los certificados:

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

[2] Ap 6.2.4.a) vi) de ETSI EN 319 411-1

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

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

CA	Frecuencia de emisión días	Duración
AC CAMERFIRMA 2009	365 días	365 días
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 Autoridad 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:

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

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Autoridad 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 Autoridad 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.

Los servicios de comprobación de estado de los certificados son de uso gratuito[3].

La AC-OMC mantiene disponible la información del estado de revocación pasado el período de validez del certificado[4].

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.

[3] Ap 6.3.10 de ETSI EN 319 411-2
[4] Ap 6.3.10.b) de ETSI EN 319 411-2

4.9.11 Otras formas de información de revocación de certificados

La Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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:

- La persona física identificada en el certificado del certificado (médico, personal administrativo, etc)

- El suscriptor del certificado (Colegio de Médicos, , etc)
- La Autoridad 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 Autoridad 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 Autoridad de Certificación de la OMC procede a la suspensión del certificado.

Se informa al suscriptor y, todo caso, a la persona física identificada en el certificado., acerca del cambio de estado del certificado suspendido.

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 Autoridad 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 Autoridad 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 Autoridad 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 "Camerfirma-CPS_eidas_v1_2". Camerfirma cumple con los controles declarados en dicha 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.

Más información en la sección 5 de la "Camerfirma-CPS_eidas_v1_2".

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 una Entidad del ámbito sanitario.

5.1 Controles de seguridad física

Dominio de creación de certificados

La Autoridad 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.

Más información en los apartados 5.1.x de la "Camerfirma-CPS_eidas_v1_2" .

Dominio de registro de usuarios y gestión de tarjetas por entidad interna
La Autoridad 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 Autoridad de Certificación de la OMC.

La Autoridad 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.
Más información en los apartados 5.1.x de la "Camerfirma-CPS_eidas_v1_2" .

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

Más información en el apartados 5.1.2 de la "Camerfirma-CPS_eidas_v1_2" .

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

Más información en el apartados 5.1.3 de la “Camerfirma-CPS_eidas_v1_2” .

5.1.4 Exposición al agua

Dominio de creación de certificados

La Autoridad de Certificación de la OMC, en las instalaciones de la subcontratada AC Camerfirma, están ubicadas en una zona de bajo riesgo de inundación.

Más información en el apartados 5.1.4 de la “Camerfirma-CPS_eidas_v1_2” .

5.1.5 Prevención y protección de incendios

Dominio de creación de certificados

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

Más información en el apartado 5.1.5 de la “Camerfirma-CPS_eidas_v1_2” .

.

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

Todas las instalaciones y activos de la Autoridad 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.

Más información en el apartado 5.1.6 de la “Camerfirma-CPS_eidas_v1_2” .

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.

Más información en el apartado 5.1.7 de la “Camerfirma-CPS_eidas_v1_2” .

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.

Más información en el apartados 5.1.8 de la “Camerfirma-CPS_eidas_v1_2” .

5.2 Controles de procedimientos

Dominio de creación de certificados

La Autoridad 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 Autoridad 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 Autoridad 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.
- Administrador de Sistemas.
- Administrador de AC.
- Operador de AC.
- Administrador de AR.
- Operador de revocación.
- Responsable de Seguridad.

Más información en el apartados 5.2.1 de la “Camerfirma-CPS_eidas_v1_2” .

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

La Autoridad 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

Se garantiza al menos dos personas para realizar las tareas clasificadas como sensibles. Principalmente en la manipulación del dispositivo de custodia de las claves de AC Root y AC intermedias.

Más información en el apartados 5.2.2 de la “Camerfirma-CPS_eidas_v1_2” .

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.

Más información en el apartados 5.2.3 de la “Camerfirma-CPS_eidas_v1_2” .

5.2.4 Arranque y parada del sistema de gestión PKI

Más información en el apartados 5.2.4 de la “Camerfirma-CPS_eidas_v1_2” .

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.

Más información en el apartados 5.3.1 de la "Camerfirma-CPS_eidas_v1_2" .

Dominio de registro

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

La Autoridad 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 AC-OMC realiza dichas comprobaciones con observancia estricta del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable.

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.

Dominio de creación de certificados

Más información en el apartados 5.3.2 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de registro

La AC-OMC realiza dichas comprobaciones con observancia estricta del Reglamento general de protección de datos, y la LOPDGDD.

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 Autoridad de Certificación forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.
Más información en el apartado 5.3.3 de la “Camerfirma-CPS_eidas_v1_2” .

5.3.4 Requisitos y frecuencia de actualización formativa

Dominio de creación de certificados

Ver apartado 5.3.4 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de Registro

La Autoridad 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, de acuerdo con su plan de formación.

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

Dominio de creación de certificados

Ver apartado 5.3.6 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de Registro

La Autoridad 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
Ver apartado 5.3.7 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de Registro
Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y la requerimientos operacionales empleados por la EC OMC.

5.3.8 Suministro de documentación al personal

Dominio de creación de certificados
Ver apartado 5.3.8 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de registro
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

Dominio de creación de certificados
La Autoridad de Certificación Camerfirma bajo la que se establece la EC OMC está sujeta a las validaciones anuales de diversas normas que se identifican en el apartado 2.7 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de registro

La Autoridad de Certificación de la Organización Médica Colegial realiza las oportunas evaluaciones de conformidad para la adecuación al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y de las normas ETSI EN 319 401, ETSI EN 319 411-1 y ETSI EN 319 411-2.

La Autoridad de Certificación de la Organización Médica Colegial está sujeta a las medidas de seguridad que correspondan de conformidad con la normativa de aplicación en materia de protección de datos.

5.4.1 Tipos de eventos registrados y su frecuencia

Dominio de creación de certificados

Ver apartado 4.9.1 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de gestión de tarjetas por entidad interna.

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas (DCCF, o en inglés QSCD) que son usados por los firmantes o custodios[5].

5.4.2 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**.

Ver apartado 4.9.2 de la “Camerfirma-CPS_eidas_v1_2” .

5.4.3 Protección de los registros de auditoría

Dominio de creación de certificados

[5] Ap 6.4.5.a) de ETSI EN 319 411-2

Los logs de los sistemas son protegidos de su manipulación, borrado o eliminación[6] mediante la firma de los ficheros que los contienen y el acceso reservado sólo a las personas autorizadas.
Ver apartado 4.9.3 de la "Camerfirma-CPS_eidas_v1_2" .

5.4.4 Procedimientos de copia de respaldo

Dominio de creación de certificados
Ver apartado 4.9.4 de la "Camerfirma-CPS_eidas_v1_2" .

5.4.5 Localización del sistema de acumulación de registros de auditoría

Dominio de creación de certificados
Ver apartado 4.9.5 de la "Camerfirma-CPS_eidas_v1_2" .

5.4.6 Notificación del evento de auditoria al causante del evento

Dominio de creación de certificados
Ver apartado 4.9.6 de la "Camerfirma-CPS_eidas_v1_2" .

5.4.7 Análisis de vulnerabilidades

Dominio de creación de certificados
Ver apartado 4.9.7 de la "Camerfirma-CPS_eidas_v1_2" .

5.5 Archivo de informaciones

Para todos los dominios
La Autoridad 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.

[6] Ap 7.10.f) de ETSI EN 319 401

5.5.1 Tipos de registros archivados

Dominio de creación de certificados

Ver apartado 4.10.1 de la “Camerfirma-CPS_eidas_v1_2” .

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

La Autoridad 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.
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al poceso de revocación[7].
- Todas aquellas elecciones específicas que el firmante o el subscriptor disponga durante el acuerdo de subscripción[8].

5.5.2 Periodo de conservación de registros

Para todos los dominios

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

Ver apartado 4.10.2 de la “Camerfirma-CPS_eidas_v1_2” .

5.5.3 Protección del archivo

Para todos los dominios

La Autoridad 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.

[7] Ap 6.4.5.h) de ETSI EN 319 411-1

[8] Ap 6.4.5.c) iv) de ETSI EN 319 411-1

Ver apartado 4.10.3 de la “Camerfirma-CPS_eidas_v1_2” .

5.5.4 Procedimientos de copia de respaldo

Dominio de creación de certificados
Ver apartado 4.10.4 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
La Autoridad 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 Autoridad de Certificación, en la entidad interna, guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Autoridad de Certificación.

5.5.5 Requisitos de sellado de fecha y hora

La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día[9].

No es necesario que esta información se encuentre firmada digitalmente.

Dominio de creación de certificados
Ver apartado 4.10.5 de la “Camerfirma-CPS_eidas_v1_2” .

[9] Ap 7.10.d) de la ETSI EN 319 401

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
Las bases de datos de la Autoridad de Certificación emplean registros fiables de fecha y hora.

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

Ver apartado 3.2 y 4.11 de la “Camerfirma-CPS_eidas_v1_2” .

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
Ver apartado 6.8.2 de la “Camerfirma-CPS_eidas_v1_2” .

Dominio de registro de usuarios y gestión de tarjetas por entidad interna.
Se guardan copias de seguridad de la siguiente información de la Autoridad de Certificación, en instalaciones de almacenamiento externo a la Autoridad 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
Ver apartado 6.8.2 de la "Camerfirma-CPS_eidas_v1_2" .

5.7.3 Compromiso de la clave privada de la entidad

En caso de compromiso de la clave privada de la entidad puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos[10].

Dominio de creación de certificados
Ver apartado 4.12 de la "Camerfirma-CPS_eidas_v1_2" .

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
Ver apartado 4.12 de la "Camerfirma-CPS_eidas_v1_2" .

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
La AC-OMC dispone de un plan de desastre para este ámbito.

[10] Ap 6.4.8.g) ii) de ETSI EN 319 411-1

5.8 Terminación del servicio

Dominio de creación de certificados

Ver apartado 4.13 de la “Camerfirma-CPS_eidas_v1_2” .

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

La Autoridad 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 Autoridad 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.
- Comunicará al Ministerio de Industria, Energía y Turismo, con una antelación mínima de 2 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también al Ministerio de Industria, Energía y Turismo, la apertura de cualquier proceso concursal que se siga contra la AC-OMC así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6 Controles de seguridad técnica

La Autoridad 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

- Ver apartado 6.1.1 de la “Camerfirma-CPS_eidas_v1_2” .

SUBCA CONSEJO GENERAL DE COLEGIOS DE MÉDICOS DE ESPAÑA	**4.096 bits**	**10 Años**
- Los certificados de entidad final	**2.048 bits**	**3 años**

Más información en las siguientes direcciones web:

Texto de divulgación o PDS	https://certificacion.cgcom.es/pds/

6.1.1.1 Generación del par de claves del firmante/suscriptor

Las claves del Firmante/Suscriptor pueden ser creadas por él mismo mediante dispositivos hardware o software autorizados por la AC OMC o pueden ser creadas por la AC OMC**.**
Las claves son generadas usando el algoritmo de clave pública **SHA-2**.
Las claves tienen una longitud mínima de **2048 bits**.

- Más información en el apartado 6.1.1.1 de la “Camerfirma-CPS_eidas_v1_2” .

Cuando la AC-OMC distribuya los dispositivos cualificados de creación de firma, verifica en todo momento que dichos dispositivos continuan certificados como un DCCF[11].
La verificación de la certificación del DCCF se realiza durante todo el período de validez del certificado[12]. Si el DCCF perdiera su certificación como tal, la AC-OMC avisará a los usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos.

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 Autoridad de Certificación de la OMC. La tarjeta es almacenada y distribuida de forma segura por la Autoridad 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.

[11] Ap 6.5.1.a) de ETSI 319 411-2
[12] Ap 6.5.1.c) de ETSI EN 319 411-2

Cuando las claves se generan en un DCCF, la AC-OMC se asegura que la clave pública que se remite al prestador de servicios de certificación proviene de un par de claves generadas por dicho DCCF[13].

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

Las claves de la Autoridad 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 Autoridad 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 = 4096
- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-1, SHA256.

[13] Ap 6.5.1.b) de ETSI EN 319 411-2

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 cualificada 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
CHAMBERS OF COMMERCE ROOT - 2016						X	X		
SUBCA CONSEJO GENERAL DE COLEGIOS DE MÉDICOS DE ESPAÑA						X	X		
Certificado corporativo de colegiado (persona física) para identificación	X								

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

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
Certificado de cifrado en tarjeta, para órgano colegial			X						
Certificado corporativo de órgano colegial (persona física), en software, para identificación, firma y cifrado	X	X	X						
Certificado corporativo de representante legal de persona jurídica para identificación	X								
Certificado corporativo de representante legal de persona jurídica para firma		X							
Certificado de cifrado en tarjeta, para representante legal de persona jurídica			X						
Certificado corporativo de representante legal de persona jurídica en software, para identificación, firma y cifrado	X	X	X						
Certificado de sello electrónico en DCCF	X	X	X						
Certificado de sello electrónico en software	X	X	X						

6.2 Protección de la clave privada

Clave privada de la 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**.

- Más información en el apartado 6.2 de la "Camerfirma-CPS_eidas_v1_2" .

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 Autoridad de Certificación de la OMC ofrecerá las instrucciones de configuración adecuada para un uso seguro en las aplicaciones reconocidas.

- Más información en el apartado 6.2 de la "Camerfirma-CPS_eidas_v1_2" .

.

6.2.1 Estándares de módulos criptográficos

- Más información en el apartado 6.2 de la "Camerfirma-CPS_eidas_v1_2" .

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

- Más información en el apartado 6.3 de la "Camerfirma-CPS_eidas_v1_2" .

6.2.3 Depósito de la clave privada

La EC OMC no almacena ni copia claves privadas de los firmantes cuando estas son generadas por el PSC. 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 firmante cuando esta se use "exclusivamente" para cifrado de datos..

6.2.4 Copia de respaldo de la clave privada

- Ver apartado 6.3.3 de la “Camerfirma-CPS_eidas_v1_2” .

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.

- Más información en el apartado 6.3 de la “Camerfirma-CPS_eidas_v1_2” .

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 Autoridad de Certificación de la OMC, en las tarjetas colegiales o en los sistemas informáticos de los suscriptores.

- Más información en el apartado 6.3 de la “Camerfirma-CPS_eidas_v1_2” .

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8 Método de activación de la clave privada

La clave privada de la Autoridad 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.

- Más información en el apartado 6.5 de la “Camerfirma-CPS_eidas_v1_2” .

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 AC-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.

- Más información en el apartado 6.3.5 de la “Camerfirma-CPS_eidas_v1_2” .

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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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.

- Más información en el apartado 6.7 de la “Camerfirma-CPS_eidas_v1_2” .

6.5.1 Requisitos técnicos específicos de seguridad informática

- Ver el apartado 6.7 de la “Camerfirma-CPS_eidas_v1_2” .

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Autoridad de Certificación de la OMC son fiables.

- Más información en el apartado 6.7 de la “Camerfirma-CPS_eidas_v1_2” .

6.6 Controles técnicos del ciclo de vida

- Más información para los controles aplicables a la AC Camerfirma en el apartado 6.8 de la “Camerfirma-CPS_eidas_v1_2” .

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por la Autoridad 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

- Ver el apartado 6.8.2.5 de la “Camerfirma-CPS_eidas_v1_2” .

6.6.3 AC-OMC Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación.

6.7 Controles de seguridad de red

- Ver el apartado 6.9 de la “Camerfirma-CPS_eidas_v1_2” .

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

- Ver el apartado 6.11 de la “Camerfirma-CPS_eidas_v1_2” .

AC-OMC

6.9 Fuentes de Tiempo

- Ver el apartado 6.10 de la “Camerfirma-CPS_eidas_v1_2” .

7 AC-OMC Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

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

Todos los certificados cualificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3, con la RFC 5280 y con ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3 y ETSI EN 319 412-5.

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:

- 1.2.840.113549.1.1.11 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.

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 raíz 1.3.6.1.4.1.26852, de acuerdo con la estructura indicada en el punto 1.2.1

7.2 Perfil de la lista de revocación de certificados

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

- Más información en el apartado 7.2 y 7.3 de la “Camerfirma-CPS_eidas_v1_2” .

7.2.1 Número de versión

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

7.2.2 Perfil de OCSP

Según el estándar IETF RFC 6960.

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.

- Más información en el apartado 2.7 de la “Camerfirma-CPS_eidas_v1_2” .

Del mismo modo, EC OMC se encuentra registrada como prestador cualificado 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

La AC 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.

- Más información en el apartado 2.7.1 de la “Camerfirma-CPS_eidas_v1_2” .

8.2 Identificación y calificación del auditor

Las auditorías de la AC-OMC 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.

- Más información en el apartado 2.7.2 de la “Camerfirma-CPS_eidas_v1_2” .

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.

- Más información en el apartado 2.7.3 de la “Camerfirma-CPS_eidas_v1_2” .

8.4 Listado de elementos objeto de auditoria

- Más información en el apartado 2.7.4 y siguientes de la “Camerfirma-CPS_eidas_v1_2” .

En cuanto a la AC-OMC los elementos de auditoría son:

- Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.
- 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.
- Que la entidad gestiona de forma adecuada sus sistemas de información

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 Autoridad 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 Autoridad de Certificación, y regenerar la infraestructura.
- Terminar el servicio de la Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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, según lo establecido en la ETSI EN 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

La Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, 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 de la persona física identificada en el certificado, 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 Autoridad 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, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa[14], 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.

[14] Apartado 7.10.c) de la ETSI EN 319 401

La Autoridad 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 Autoridad 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, de la persona física identificada en el certificado, 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 Autoridad 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, con cumplimiento estricto de las condiciones para el tratamiento legítimo a que se refiere el artículo 6 Reglamento general de protección de datos, y concordantes de la LOPDGDD.

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

La Autoridad de Certificación ha desarrollado una política de intimidad y documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes de conformidad con el Reglamento general de protección de datos, y la LOPDGDD.

La Autoridad 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, del presente documento, en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la normativa en protección de datos personales, es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en este documento en cumplimiento del Reglamento general de protección de datos, y la LOPDGDD.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

La Autoridad 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 la documentación que los vincula.

Adicionalmente, los certificados emitidos por la Autoridad 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 Autoridad 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, la persona física identificada en el certificado, 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 Autoridad de Certificación de la OMC

La Autoridad 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 Autoridad 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 Autoridad 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 o PDS (PKI Disclosure Statement)” aplicable, que cumple el contenido del anexo A de la ETSI EN 319 411-1, documento que puede ser transmitido electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

La AC-OMC comunicará de forma permanente los cambios[15] que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en el apartado "Regulación" de su página web https://certificacion.cgcom.es.

La Autoridad de Certificación vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante el Texto de Divulgación-PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.4, 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 cualificado 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 Autoridad 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 Autoridad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Autoridad 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 Autoridad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

[15] Ap 6.2.3.b) de ETSI EN 319 411-1

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

La Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad de Certificación garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado de acuerdo con el Reglamento (UE) 910/2014, en su anexo I para certificados cualificados de firma y en su anexo III para certificados cualificados de sello electrónico.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado., se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan.

9.6.3 Rechazo de otras garantías

La Autoridad 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 Autoridad 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 Autoridad de Certificación.

9.6.5 Cláusulas de indemnidad

9.6.5.1 Cláusula de indemnidad de suscriptor

La Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad 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 Autoridad de Certificación de la OMC incluye cláusulas en los textos de divulgación-PDS para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7 Ley aplicable

La Autoridad de Certificación establece, en el contrato de suscriptor y enlos textos de divulgación-PDS, 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 Autoridad 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 Autoridad 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 Autoridad de Certificación de la OMC establece, en los textos de divulgación-PDS, 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 Autoridad de Certificación de la OMC establece, en los textos de divulgación-PDS, los procedimientos de mediación y resolución de conflictos aplicables.