Declaración de Prácticas de Certificación

Entidad de Certificación de la Organización Médica Colegial

Tabla de contenido

1. Introducción

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

1) La regulación de la emisión y gestión de la tarjeta de médico colegiado, con la condición de dispositivo seguro de creación de firma electrónica.

2) La emisión y gestión, por uno o más prestadores de servicios de certificación, de certificados reconocidos de firma electrónica de médico colegiado y otro personal colegial, así como de otros servicios de certificación, que se prestarán sobre la tarjeta de médico.

3) La acreditación, por la Organización Médica Colegial, de los diferentes prestadores de servicios de certificación que suministren certificados a los profesionales colegiados, al objeto de garantizar la calidad y seguridad en la emisión y gestión de los citados certificados.

4) La prestación de servicios de validación y re-certificación a entidades, públicas y privadas, sobre los certificados, al objeto de garantizar la actualidad y validez de las informaciones corporativas, incluidas o no en los certificados, y en especial, de la condición de médico.

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

Todo ello se realiza sobre la base de la tarjeta médica colegial, único y exclusivo 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.

A) Presentación

Este documento declara las prácticas de certificación de firma electrónica de la Entidad de Certificación de la Organización Médica Colegial, que se basa en la tarjeta colegial.

Los certificados que se emiten son los siguientes:

- Certificado corporativo de médico/a colegiado/a.
- Certificado corporativo de órgano colegial.
- Certificado corporativo de personal administrativo.
- Certificado corporativo de colegio profesional.

Los servicios de certificación prestados por la Entidad de Certificación de la OMC se encuentran integrados en la red mundial VeriSign Trust Network, 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.

La integración de la Entidad de Certificación de la OMC dentro de la red mundial de VeriSign se ha realizado mediante la firma del certificado de la Entidad de Certificación de la OMC, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación de la VeriSign Trust Network v3.2, de 1 de mayo de 2006, a la que se sujeta la presente Declaración.

Los certificados incluyen las oportunas menciones a las condiciones de uso y a la Declaración de Prácticas de Certificación de VeriSign.

B) Nombre del documento e identificación

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

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	**Identificador de objeto**
	1.3.6.1.4.1.26852.1 + el siguiente valor:
Certificados corporativos	.1
Certificados de colegiado	.1.1
Certificados de personal administrativo	.1.2
Certificados de persona jurídica	.1.3
Certificado de órgano colegial	.1.4

Los certificados incluyen, además, los identificadores de política de certificados de clase 2 asignados dentro de la VeriSign Trust Network, en la que se integran estos certificados.

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

En este momento no se expiden certificados externos.

C) 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.

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

1. Prestador de Servicios de Certificación

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

El papel de la Organización Médica Colegial es doble:

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

2. Registradores

En general, los registradores de certificados corporativos son las entidades de la Organización Médica Colegial, y en especial, los Colegios de Médicos.

La Organización Medica Colegial dispone de un Sistema Unificado de Registro (SUR) de los diferentes Colegios, operado por la sociedad mercantil e-OMC, mediante el cual se asiste técnicamente en el registro a los Colegios de Médicos.

3. Entidades finales

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

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

1) Solicitantes de certificados.

2) Suscriptores de certificados.

3) Poseedores de claves.

4) Terceros que confían en certificados.

a) 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.

2) Una persona autorizada por dicho futuro suscriptor.

b) Suscriptores de certificados

Los suscriptores son los colegios identificados en los certificados.

El suscriptor tiene licencia de uso del certificado, y actúa siempre a través de un poseedor de claves, debidamente autorizado, y que figura identificado en el certificado.

c) Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves de firma digital y de descifrado, pudiendo ser colegiados/as, personal administrativo, órganos colegiales y custodios de certificados colegiales.

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

La clave privada de descifrado no puede ser recuperada por el prestador de servicios de certificación, por lo que los poseedores de claves son los únicos responsables de su protección y deberían considerar las implicaciones de perder una clave privada de descifrado, dado que puede implicar la pérdida de documentos cifrados.

d) Terceros que confían en certificados

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

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

4. Otros participantes

a) Proveedores técnicos

Los servicios de certificación prestados por la Entidad de Certificación de la OMC se apoyan en los siguientes proveedores técnicos:

- VeriSign Inc, que colabora en la generación técnica de los certificados, desde sus instalaciones de alta seguridad.
- e-OMC, que colabora en los procesos de registro y emisión técnica de los certificados.

b) Jerarquías externas de certificación

Como se ha indicado anteriormente, los certificados se integran en la VeriSign Trust Network.

D) 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. Usos permitidos para los certificados

a) Certificado corporativo de colegiado/a

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

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

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

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

Asimismo 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.

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

a) Autenticación en sistemas de control de acceso.

b) Firma de correo electrónico seguro.

c) Otras aplicaciones de firma digital.

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

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

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

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

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

b) Certificado corporativo de personal administrativo

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

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

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

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

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

poseedor mediante otros medios, diferentes al certificado, como por ejemplo el servicio de validación de la OMC.

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

a) Autenticación en sistemas de control de acceso.

b) Firma de correo electrónico seguro.

c) Otras aplicaciones de firma digital.

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

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

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

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

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

c) Certificado corporativo de colegio profesional

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

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

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

Los certificados corporativos de colegio profesional garantizan la identidad del subscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

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

a) Autenticación en sistemas de control de acceso.

b) Firma de correo electrónico seguro.

c) Otras aplicaciones de firma digital.

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

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

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

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

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

d) Certificado corporativo de órgano colegial

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

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

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

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

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

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

a) Autenticación en sistemas de control de acceso.

b) Firma de correo electrónico seguro.

c) Otras aplicaciones de firma digital.

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

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

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

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

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

2. Límites y prohibiciones de uso de los certificados

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

Del mismo modo, los certificados deberán 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.

E) Administración de la política

1. Organización que administra el documento

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS DE ESPAÑA – ORGANIZACIÓN MÉDICA COLEGIAL

PLAZA DE LAS CORTES, 11- 28014 MADRID

TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

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

3. Procedimientos de gestión del documento

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

2. Publicación de información y depósito de certificados

A) Depósito(s) de certificados

La Entidad de Certificación de la OMC dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la Entidad de Certificación de la OMC, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.G)4 de esta Declaración de Prácticas de Certificación.

B) Publicación de información del prestador de servicios de certificación

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

- Los certificados emitidos.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.
- Las condiciones generales de la contratación aplicables a los suscriptores y a los terceros que confían en certificados.

C) 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 los documentos de política y en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.E) de esta Declaración de Prácticas de Certificación.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.I)7 y 4.I)8 de esta Declaración de Prácticas de Certificación.

D) Control de acceso

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

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

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

3. Identificación y autenticación

A) Registro inicial

1. Tipos de nombres

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

Los nombres contenidos en los certificados son los siguientes.

a) Certificado corporativo de colegiado/a

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

b) Certificado corporativo de personal administrativo

Country (C)	"ES"
Organization (O)	Colegio profesional
Organizational Unit (OU)	"Condiciones de uso en

	https://www.cgcom.es/CertAdmin (c)06”
Surname	Apellidos
Given Name	Nombre
Title	"Personal administrativo y de servicios”
Serial Number	DNI/NIE
Common Name (CN)	Nombre y apellidos

c) Certificado corporativo de colegio profesional

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

d) Certificado corporativo de órgano colegial

Country (C)	“ES”
Organization (O)	Colegio profesional
Organizational Unit (OU)	“Condiciones de uso en https://www.cgcom.es/CertOrg (c)06”
Surname	Apellidos
Given Name	Nombre

Title	Órgano o cargo
Serial Number	DNI/NIE
Common Name (CN)	Nombre y apellidos

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. Empleo de anónimos y seudónimos

En ningún caso se pueden emplear anónimos ni seudónimos.

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 y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

El campo “número de serie” debe incluir el DNI o el NIE del colegiado, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

En el caso de los certificados de colegio profesional, de acuerdo con la normativa tributaria, el campo "número de serie" debe incluir el NIF de la persona jurídica, mientras que el campo identificado con el número "1.3.6.1.4.1.18838.1.1", debe incluir el DNI o el NIE del custodio.

5. Unicidad de los nombres

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

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia

del número del Documento Nacional de Identidad, o equivalente, en el esquema de nombres.

6. Resolución de conflictos relativos a nombres

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

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

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

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

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

B) Validación inicial de la identidad

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

A estos efectos, la Organización Médica Colegial dispone del Sistema Unificado de Registro (SUR), que garantiza la corrección y consistencia de las informaciones contenidas en dichos registros corporativos.

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

1. Prueba de posesión de clave privada

El par de claves es generado por la Entidad de Certificación de la OMC, en su caso asistido por las entidades indicadas en la sección 1.C)4.a) 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 dispositivo seguro y del correspondiente certificado y par de claves almacenados en su interior.

2. Autenticación de la identidad de una organización

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.

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

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.

Los registros colegiales integrados en el Sistema de Registro Unificado (SUR) son los únicos que legalmente permiten acreditar la condición de colegiado/a, órgano colegial, personal administrativo o colegio profesional.

Por este motivo, la información de identificación de poseedores de claves de certificados corporativos se valida comparando la información de la solicitud con los registros del Colegio correspondiente, asegurando la corrección de la información a certificar.

a) Necesidad de presencia personal

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

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

Durante este trámite, que puede diferirse al momento de entrega y aceptación del certificado y del dispositivo seguro de creación de firma, se confirma la validación de la identidad de la persona.

b) Vinculación de la persona física con una organización

Dado que se trata de certificados corporativos, la justificación documental de la vinculación del poseedor de la clave con el Colegio es la propia solicitud y el certificado administrativo que la acompaña.

4. Información de suscriptor no verificada

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

C) Identificación y autenticación de solicitudes de renovación

1. Validación para la renovación rutinaria de certificados

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

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de renovación por parte del suscriptor, acompañada del correspondiente certificado administrativo.
- El uso de una "frase de comprobación de identidad", que consiste en información que sólo conoce el poseedor de claves, y que le permite renovar de forma automática su certificado.
- El empleo del certificado vigente para su renovación, en los términos legalmente establecidos.

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.B).

2. Validación para la renovación de certificados tras la revocación

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado, la Entidad de Certificación de la OMC comprueba que la información empleada para

verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.

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

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

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.B).

D) Identificación y autenticación de la solicitud de revocación

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

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor, firmada electrónicamente.
- El uso de la "frase de comprobación de identidad", que consiste en información que sólo conoce el poseedor de claves, y que le permite revocar de forma automática su certificado.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de la Entidad de Certificación de la OMC.

4. Requisitos de operación del ciclo de vida de los certificados

A) Solicitud de emisión de certificado

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.

2. Procedimiento de alta; Responsabilidades

Existen los siguientes tipos de solicitudes:

1) Solicitud electrónica de certificado de oficio (no contiene clave pública, ni se encuentra firmada digitalmente).

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

La Entidad de Certificación de la OMC recibe solicitudes de certificados, realizadas de oficio por las entidades que integran la Organización Médica Colegial, o 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 a la Entidad de certificación, el cual incluirá la indicación de la persona o personas a autorizar para realizar peticiones, así como, en su caso, los datos de las personas a las que se expedirán certificados.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias del poseedor de claves, de acuerdo con lo establecido en la sección 3.B)3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar al poseedor de claves.

Asimismo, el Colegio acepta un convenio de suscriptor, en forma de condiciones generales de emisión.

B) Procesamiento de la solicitud de certificación

1. Ejecución de las funciones de identificación y autenticación

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

En caso afirmativo, la Entidad de Certificación de la OMC verifica la información proporcionada, verificando los aspectos descritos en la sección 3.B).

2. Aprobación o rechazo de la solicitud

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

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, la Entidad de Certificación de la OMC deniega la petición, o detiene su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, se deniega la solicitud definitivamente.

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

3. Plazo para resolver la solicitud

La Entidad de Certificación de la OMC atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

C) Emisión del certificado

1. Acciones de la Entidad de Certificación de la OMC durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado y grabación en la tarjeta, de forma segura y se pone la misma a disposición del suscriptor, que la entrega al poseedor de claves para su aceptación, de acuerdo con lo establecido en la sección 4.C)2.

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

La Entidad de Certificación de la OMC:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves, y almacena la clave privada de forma segura y el correspondiente certificado en la tarjeta del poseedor de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de 19 de diciembre, de acuerdo con lo establecido en las secciones 3.A)1 y 7.A).
- Indica la fecha y la hora en que se expidió un certificado.
- Emplea un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al suscriptor.

2. Notificación de la emisión al suscriptor

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

D) Entrega y aceptación del certificado

1. Responsabilidades de la Entidad de Certificación de la OMC

La Entidad de Certificación:

- Acredita definitivamente la identidad del poseedor de claves, con la colaboración del suscriptor, de acuerdo con lo establecido en las secciones 3.B)2 y 3.B)3.
- Entrega al poseedor de claves, con la colaboración del suscriptor, la tarjeta que contiene el certificado.
- Entregar al poseedor de claves, con la colaboración del suscriptor, una hoja de entrega y aceptación de la tarjeta y el correspondiente certificado, 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 de la tarjeta.

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

  d) Obligaciones del poseedor de claves.

  e) Responsabilidad del poseedor de claves.

  f) Método de imputación exclusiva al poseedor de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones 6.B) y 6.D).

  g) La fecha del acto de entrega y aceptación.

El suscriptor colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y remitir los citados documentos originales a la Entidad de Certificación de la OMC.

Para ello, la Entidad de Certificación de la OMC remite al suscriptor el paquete de tarjetas solicitadas, junto con las hojas de entrega y aceptación correspondientes, y

remite directamente a cada poseedor de claves sus datos de activación de firma y otras informaciones.

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

2. Conducta que constituye aceptación del certificado

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

Cuando el poseedor de claves ha aceptado el certificado y la tarjeta, puede acceder a la misma con los datos de activación recibidos y producir firmas electrónicas.

3. Publicación del certificado

La Entidad de Certificación de la OMC publica el certificado en el Depósito a que se refiere la sección 2.A), con los controles de seguridad pertinentes.

4. Notificación de la emisión a terceros

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

E) Uso del par de claves y del certificado

1. Uso por el suscriptor

a) Obligaciones del suscriptor del certificado

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

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.D).

- Reconocer su capacidad de producción de firmas electrónicas reconocidas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.A), 6.B) y 6.D).
- Comunicar a la Entidad de Certificación y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:

  a) La pérdida, el robo o el compromiso potencial de su clave privada.

  b) La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN de la tarjeta) o por cualquier otra causa.

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

  d) La pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su tarjeta.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.C)2.
- Imponer a los poseedores de claves el cumplimiento de las obligaciones específicas de los mismos.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Entidad de Certificación de la OMC, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación del prestador de servicios de certificación de la Entidad de Certificación de la OMC, sin permiso previo por escrito.

b) Responsabilidad civil del suscriptor de certificado

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

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.

- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del suscriptor, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni a título de prestador de servicios de certificación ni en ningún otro caso.

2. Uso por el tercero que confía en certificados

a) Obligaciones del tercero que confía en certificados

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

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

b) Responsabilidad civil del tercero que confía en certificados

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

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

F) 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.G).

G) Renovación de claves y certificados

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.

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.

3. Procedimientos de solicitud de renovación

a) Realización de la solicitud

La Entidad de Certificación de la OMC recibe solicitudes de certificados, realizadas de oficio por las entidades que integran la Organización Médica Colegial, o 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 a la Entidad de certificación, el cual incluirá la indicación de la persona o personas a autorizar para realizar peticiones, así como, en su caso, los datos de las personas a las que se expedirán certificados.

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

Asimismo, el Colegio acepta un convenio de suscriptor, en forma de condiciones generales de emisión.

b) 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.

c) Aprobación o rechazo de la solicitud

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

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

d) Plazo para resolver la solicitud

La Entidad de Certificación de la OMC atiende las solicitudes de renovación certificados por orden de llegada, en un plazo razonable anterior a la expiración de los certificados a revocar, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.

Las solicitudes de renovación se mantienen activas hasta su aprobación o rechazo.

4. Notificación de la emisión del certificado renovado

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

5. Conducta que constituye aceptación del certificado

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

Cuando el poseedor de claves ha aceptado el certificado y la tarjeta, puede acceder a la misma con los datos de activación recibidos y producir firmas electrónicas.

6. Publicación del certificado

La Entidad de Certificación de la OMC publica el certificado renovado en el Depósito a que se refiere la sección 2.A), con los controles de seguridad pertinentes.

7. Notificación de la emisión a terceros

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

H) 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.A), 4.B), 4.C) y 4.D).

I) Revocación y suspensión de certificados

Esta sección detalla las prácticas relativas a la revocación de certificados; esto es, la finalización anticipada y definitiva de la validez de los certificados.

La Entidad de Certificación de la OMC no presta servicios de suspensión temporal de la validez de los certificados, y por lo tanto este documento no contiene las secciones correspondientes a esta práctica.

1. Causas de revocación de certificados

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

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

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

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

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

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

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

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

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

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

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

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

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

b) Pérdida o inutilización por daños de la tarjeta.

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

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

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

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

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

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

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

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

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.D).

5) Otras circunstancias:

a) La terminación del servicio de certificación de la OMC, de acuerdo con lo establecido en la sección 5.H).

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

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

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

3º) La legislación relevante vigente en cada momento.

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

2. Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

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

3. Procedimientos de solicitud de revocación

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

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

En aquellos casos en que se requiera revocación inmediata del certificado, se podrá hacer una llamada o enviar un correo electrónico a:

[Datos de contacto telefónico]
[Datos de contacto e-mail]

La solicitud debe ser autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 3.D) de esta política, antes de proceder a la revocación.

En caso de que el destinatario de la solicitud fuera el registrador, una vez autenticada, debe remitir una solicitud en este sentido a la Entidad de Certificación de la OMC.

La solicitud de revocación será procesada a su recepción.

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

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

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.

5. Plazo temporal de procesamiento de la solicitud

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

6. Obligación de consulta de información de revocación de certificados

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

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de la OMC.

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

http://crl1.cgcom.es/crl/ec-cgcom.crl

http://crl2.cgcom.es/crl/ec-cgcom.crl

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

7. Frecuencia de emisión de listas de revocación de certificados (LRCs)

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

La 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.

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.

9. Disponibilidad de servicios de comprobación en línea de estado de certificados

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

La dirección electrónica del Depósito es:

https://www.cgcom.es/deposito

Asimismo, la Entidad de Certificación de la OMC dispone de un servicio web para la consulta de los certificados que han sido recientemente revocados. Dicho servicio web sigue la especificación de la AEAT publicada en la dirección electrónica https://aeat.es/ycaestec.html.

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

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

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.

11. Otras formas de información de revocación de certificados

La Entidad de Certificación de la OMC no implanta otras formas de provisión de información acerca del estado de revocación de los certificados.

12. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de la Entidad de Certificación de la OMC es notificado, en la medida de lo posible, a todos los participantes en los servicios de certificación de la OMC, mediante la publicación de este hecho en la página web de la OMC, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

J) Finalización de la suscripción

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

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

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

K) Servicios de comprobación de estado de certificados

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.

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.

3. Características opcionales

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

L) Depósito y recuperación de claves

1. Política y prácticas de depósito y recuperación de claves

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

2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5. Controles de seguridad física, de gestión y de operaciones

A) Controles de seguridad física

La Entidad de Certificación de la OMC 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.

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

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

1. Localización y construcción de las instalaciones

La Entidad de Certificación de la OMC dispone de instalaciones que protegen físicamente la prestación de los servicios de generación de certificados, de gestión 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.

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 fuera bruta.

La Entidad de Certificación de la OMC también mantiene instalaciones de recuperación ante desastre para sus operaciones de generación de certificados, con perímetros de seguridad comparables a los de las instalaciones principales.

2. Acceso físico

La Entidad de Certificación de la OMC dispone de un mínimo de cuatro niveles de seguridad física, debiendo accederse desde los niveles inferiores a los niveles superiores.

Para el acceso a las dependencias del prestador de servicios de certificación donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, que se realizan en los niveles más restrictivos, es necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Esta identificación, ante el sistema de control de accesos, deberá realizarse mediante técnicas de doble factor de autenticación, incluyendo una tarjeta de proximidad de empleado y el reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de los prestadores de servicios de certificación, así como su almacenamiento, se realiza en niveles específicos para estos fines, incluyendo cabinas específicas y cajas fuertes, que requieren de acceso con autenticación de doble factor, incluyendo biometría, y permanencia duales.

Los accesos a materiales de claves se encuentran sujetos a una estricta política de segregación de funciones, y la apertura y cierre de dichas cabinas y cajas fuertes se registra para su auditoría posterior.

3. Electricidad y aire acondicionado

Los equipos informáticos de la Entidad de Certificación de la OMC se encuentran convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiere el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos se encuentran ubicados en un entorno que garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

4. Exposición al agua

La Entidad de Certificación de la OMC dispone de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso de que las condiciones de ubicación de las instalaciones lo hagan necesario.

5. Prevención y protección de incendios

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

6. Almacenamiento de soportes

Todos los medios que contienen aplicativos o datos de producción, de auditoría, de archivo o copias de respaldo se encuentran almacenados en las instalaciones de la Entidad de Certificación de la OMC y en dependencias externas seguras, con las medidas de seguridad física y de acceso diseñadas para limitar el acceso a las personas autorizadas y proteger dichos medios de daños accidentales (como inundación, incendio, etc.)

7. Tratamiento de residuos

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

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

En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

8. Copia de respaldo fuera de las instalaciones

Periódicamente, la Entidad de Certificación de la OMC almacena copia de respaldo de los datos de sistemas de información, datos de auditoría y de otras informaciones críticas, en dos dependencias seguras físicamente separadas de aquellas en las que se encuentran los equipos, una de ellas alejada geográficamente de las instalaciones principales.

B) Controles de procedimientos

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

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

1. Funciones fiables

La Entidad de Certificación de la OMC 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 de operación criptográfica.
- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Determinado personal de ingeniería.
- Auditores del sistema.

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

2. Número de personas por tarea

Las funciones fiables identificadas en la política de seguridad del prestador de servicios de certificación, y sus responsabilidades asociadas, se encuentran documentadas en descripciones de puestos de trabajo.

La Entidad de Certificación de la OMC ha establecido, mantiene y ejecuta procedimientos de control rigurosos que garantizan la segregación de funciones basada en las funciones anteriormente indicadas y que se requieren personas fiables para la realización de tareas sensibles.

Las tareas más sensibles, como el acceso y la gestión del hardware criptográfico de la Entidad de Certificación y las claves asociadas, requiere múltiples personas fiables. En concreto, los procedimientos de control interno han sido diseñados para garantizar que, como mínimo, se requieren dos personas fiables para acceder física o lógicamente al dispositivo.

El acceso al hardware criptográfico de la Entidad de Certificación por parte de múltiples personas fiables se controla de forma estricta a lo largo de todo el ciclo de vida, desde su recepción e inspección hasta su destrucción final, sea ésta física o lógica.

Una vez que un módulo es activado con claves operativas, se aplican controles adicionales para mantener control segregado sobre el acceso físico y lógico. Las personas con acceso físico a los módulos no poseen claves compartidas correspondientes a los módulos, y viceversa.

3. Identificación y autenticación para cada función

La Entidad de Certificación identifica y autentica al personal antes de asignarlo a la correspondiente función fiable, mediante los controles y procedimientos indicados posteriormente.

4. Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Validación de información en las solicitudes de certificación.
- Aceptación, rechazo y resto de procesos de la solicitud de certificación, revocación, renovación o tratamiento de las informaciones de registro.
- Emisión y revocación de certificados, y el acceso al depósito.
- La gestión de las solicitudes e informaciones de los suscriptores y poseedores de claves.
- Generación, emisión y destrucción de certificados de Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

C) Controles de personal

1. Requisitos de historial, calificaciones, experiencia y autorización

La Entidad de Certificación de la OMC emplea personal cualificado y con la experiencia necesaria, para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

Este requisito se aplica al personal de gestión del prestador de servicios de certificación, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia pueden suplirse mediante una formación y entrenamiento apropiados proporcionados por la Entidad de Certificación de la OMC.

El personal en puestos fiables debe encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

La Entidad de Certificación no puede asignar a un puesto fiable o de gestión a una persona que no sea idóneo para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, la Entidad de Certificación de la OMC realiza una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a la idoneidad del candidato.

2. Procedimientos de investigación de historial

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

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

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.
- Incumplimiento reiterado por el candidato de sus obligaciones económicas.
- Ciertas condenas penales del 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.

3. Requisitos de formación

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

Los programas de formación son actualizados y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

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

4. Requisitos y frecuencia de actualización formativa

La Entidad de Certificación de la OMC actualiza la formación del personal de acuerdo con las necesidades y la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria.

5. Secuencia y frecuencia de rotación laboral

No aplicable.

6. Sanciones para acciones no autorizadas

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

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

7. Requisitos de contratación de profesionales

La Entidad de Certificación de la OMC puede contratar profesionales para cualquier función, incluso para un puesto fiable, en cuyo caso se somete a los mismos controles que los empleados en puestos fiables.

En el caso de que el profesional no deba someterse a tales controles, debe estar constantemente acompañado por un empleado fiable, cuando se encuentra en las instalaciones de la Entidad de Certificación.

8. Suministro de documentación al personal

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.

D) Procedimientos de auditoria de seguridad

1. Tipos de eventos registrados

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

- Eventos de gestión del ciclo de vida de la clave de la Entidad de Certificación
    - Generación, copia de seguridad, almacenamiento, recuperación, archivo y destrucción de la clave.
    - Eventos de gestión del ciclo de vida de dispositivos criptográficos.
- Eventos de gestión del ciclo de vida de los certificados de la Entidad de Certificación y de los suscriptores
    - Solicitudes de emisión, renovación y revocación de certificados.
    - Procesamiento correcto e incorrecto de solicitudes.
    - Generación y emisión de certificados y listas de revocación de certificados.
- Eventos relacionados con la seguridad
    - Intentos de acceso, exitosos y no exitosos, al sistema PKI.
    - Acciones sobre el sistema PKI y el sistema de seguridad, por parte del personal de la Entidad de Certificación.
    - Lectura, escritura y borrado de ficheros y registros con información sensible de seguridad.
    - Cambios en el perfil del sistema.
    - Caídas del sistema, errores de hardware y otras incidencias.
    - Actividad de cortafuegos y routers.

- Entradas y salidas de visitantes a las instalaciones de la Entidad de Certificación de la OMC.

Las entradas del registro incluyen los siguientes elementos:

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

2. Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinan por lo menos una vez a la semana en busca de actividad sospechosa o no habitual. Asimismo, se revisan los registros en respuesta a alertas generadas por sistemas de detección.

El procesamiento de los registros de auditoría consiste en una revisión de los registros la cual incluye la verificación de que los registros no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las acciones llevadas a cabo a partir de la revisión de auditoría son documentadas.

3. Periodo de conservación de registros de auditoría

Los registros de auditoría se retienen en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivan de acuerdo con la sección 5.E)2 de esta política.

4. Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5. Procedimientos de copia de respaldo

Se generan copias incrementales de respaldo de registros de auditoría diariamente, y copias completas semanalmente.

6. Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría es un sistema interno de la Entidad de Certificación de la OMC, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que son almacenados por el personal debidamente autorizado.

7. Notificación del evento de auditoria al causante del evento

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

8. Análisis de vulnerabilidades

Los eventos en el proceso de auditoría son guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad son ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.

Estos análisis se realizan diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, de la Entidad de Certificación de la OMC.

E) Archivo de informaciones

La Entidad de Certificación de la OMC garantiza que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.E)2 de esta política.

1. Tipos de registros archivados

La Entidad de Certificación de la OMC archiva:

- Todos los datos de auditoría identificados en la sección 5.D).
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.

- Información del ciclo de vida del certificado.

2. Periodo de conservación de registros

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

3. Protección del archivo

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

Los medios que contienen los datos de archivo y las aplicaciones requeridas para su procesamiento serán mantenidos de forma que se garantice el acceso a los datos de archivo durante el periodo establecido anteriormente.

4. Procedimientos de copia de respaldo

La Entidad de Certificación de la OMC realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, y copias de respaldo completas semanalmente para casos de recuperación de datos.

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

5. Requisitos de sellado de fecha y hora

La Entidad de Certificación de la OMC emite los certificados y las listas de revocación de certificados con información fiable de fecha y hora. Asimismo, las bases de datos de la Entidad de Certificación emplean registros fiables de fecha y hora.

No es necesario que esta información se encuentre firmada digitalmente.

6. Localización del sistema de archivo

La Entidad de Certificación de la OMC dispone de sistemas de archivo internos y externos.

7. Procedimientos de obtención y verificación de información de archivo

Sólo personas autorizadas por la Entidad de Certificación de la OMC tienen acceso a los datos de archivo.

La integridad de la información es verificada cuando se restaura.

F) Renovación de claves

La renovación de las claves de la Entidad de Certificación de la OMC se realiza de acuerdo con los procedimientos descritos en la declaración de prácticas de certificación de la VeriSign Trust Network.

G) Compromiso de claves y recuperación de desastre

1. Procedimientos de gestión de incidencias y compromisos

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

Las copias de seguridad de las claves privadas de la Entidad de Certificación son generadas y mantenidas de acuerdo con lo establecido en la sección 6.B)4.

2. Corrupción de recursos, aplicaciones o datos

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

3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de la Entidad de Certificación de la OMC, se activan los procedimientos de compromiso de claves, dirigidos por un

equipo de respuesta que evalúa la situación, desarrolla un plan de acción y lo ejecuta con la aprobación de la dirección de la Entidad de Certificación.

En el caso de que deba revocarse la clave pública de la Entidad de Certificación de la OMC, se realizan las siguientes acciones:

- Se informa del hecho publicando una lista de revocación de certificados en el depósito.
- Se realizan todos los esfuerzos razonablemente necesarios para informar de la revocación a todos los suscriptores de certificados, así como a los terceros.
- Se renuevan las claves en los términos previstos en la sección 4.G), excepto cuando se proceda a la terminación del servicio, según lo establecido en la sección 5.F) de esta política.

4. Continuidad del negocio después de un desastre

La Entidad de Certificación de la OMC dispone de un centro de recuperación de desastre a más de 1600 kilómetros de distancia de las instalaciones principales de operación.

La Entidad de Certificación ha desarrollado, implementado y probado un plan de recuperación de desastres que mitiga los efectos de cualquier desastre natural o causado por el hombre. Este plan se prueba, verifica y actualiza regularmente para ser efectivo en caso de desastre.

La ubicación de los sistemas de recuperación de desastres dispone de las protecciones físicas de seguridad necesarias para el funcionamiento seguro y adecuado, en emergencia.

La Entidad de Certificación de la OMC es capaz de restaurar la operación normal de los servicios esenciales en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Emisión de certificados.
- Revocación de certificados.
- Publicación de información de revocación.

La base de datos de recuperación de desastres se encuentra sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad del prestador.

Los equipos de recuperación de desastres disponen de medidas de seguridad físicas equivalentes a las especificadas en la sección 5.A)1.

El plan de recuperación de desastres de la Entidad de Certificación de la OMC ha sido diseñado para disponer de recuperación total en el plazo de una semana desde el

desastre. Al efecto, la Entidad de Certificación dispone de y prueba el equipamiento necesario en las instalaciones principales para ofrecer las funciones de registro de usuarios y emisión de certificados después de un desastre, excepto cuando por la naturaleza del mismo la totalidad de las instalaciones quedan inoperantes. Los resultados de dichas pruebas se revisan y guardan a efectos de autoría y planificación.

Después de un desastre, las operaciones en las instalaciones principales se reanudan tan pronto como resulta posible, si ello es viable.

La Entidad de Certificación mantiene maquinaria redundante y copias de seguridad de sus programas de infraestructura de sistema y de autoridad de certificación en su centro de recuperación de desastres. Adicionalmente, se hace copia de seguridad de las claves privadas, que se mantienen en el mismo centro para la recuperación del desastre, de acuerdo con la sección 6.B)4.

La Entidad de Certificación mantiene, fuera de sus instalaciones, copias de seguridad de, al menos, las siguientes informaciones: datos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

H) Terminación del servicio

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

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

- Información a todos los suscriptores y terceros que confían en certificados, incluyendo la gestión de los costes de notificación.
- Retirada de toda autorización de subcontrataciones que actúan en nombre del prestador de servicios de certificación en el proceso de emisión de certificados.
- Revocación del certificado de la Entidad de Certificación.
- Revocación de los certificados en vigor a la terminación, incluyendo el reintegro de cantidades abonadas por los suscriptores por los certificados a revocar.
- 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.
- Destrucción de las claves privadas de la Entidad de Certificación o retirada de su uso.

6. Controles de seguridad técnica

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

A) Generación e instalación del par de claves

1. Generación del par de claves

El par de claves de la Entidad de la Certificación de la OMC es creado por la Entidad de Certificación Primaria de Clase 2 de VeriSign, de acuerdo con los procedimientos de ceremonia de claves de la VeriSign Trust Network, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

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

El par de claves es generado empleando un dispositivo criptográfico que cumple FIPS 140-2 Nivel 3.

Los pares de claves de los suscriptores se generan siempre en la tarjeta colegial, con la consideración de dispositivo criptográfico que cumple ISO 15408: EAL 4+ (o superior), de acuerdo con lo establecido en CEN CWA 14169, según proceda; o FIPS 140-2 Nivel 3 (o superior).

2. Envío de la clave privada al suscriptor

La clave privada del suscriptor se le entrega debidamente protegida mediante la entrega de la tarjeta colegial indicada anteriormente.

La preparación de la tarjeta es controlada de forma segura por la Entidad de Certificación de la OMC. La tarjeta es almacenada y distribuida de forma segura por la Entidad de Certificación de la OMC, como se indica en la sección 4.D), y la desactivación y reactivación de la tarjeta se controla de forma segura.

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 el Organización Médica Colegial.

4. Distribución de la clave pública del prestador de servicios de certificación

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

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

5. Tamaños de claves

La longitud de las claves de la Entidad de Certificación de la OMC es de 2048 bits.

6. Generación de parámetros de clave pública

Sin estipulación.

7. Comprobación de calidad de parámetros de clave pública

Sin estipulación.

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.A)1.

9. Propósitos de uso de claves

El prestador de servicios de certificación incluye las extensiones *KeyUsage* y *ExtendedKeyUsage* en los certificados, indicando los usos permitidos de las correspondientes claves privadas, de acuerdo con lo establecido en la sección 7.A).

B) Protección de la clave privada

1. Estándares de módulos criptográficos

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

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

El acceso a las claves privadas de la Entidad de Certificación requiere necesariamente del concurso simultáneo de tres (3) dispositivos criptográficos protegidos por una clave de acceso.

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

3. Depósito de la clave privada

La Entidad de Certificación de la OMC no realiza depósito de ninguna clave privada, ni la Entidad de Certificación ni de los suscriptores.

4. Copia de respaldo de la clave privada

La clave privada de la Entidad de Certificación de la OMC cuenta con una copia de respaldo para recuperación rutinaria o en caso de desastre. Dicha clave es almacenada en forma cifrada dentro de módulos criptográficos y dispositivos asociados de almacenamiento de claves. Los citados módulos cumplen los estándares establecidos en este documento. La clave privada es copiada a los módulos criptográficos de seguridad de acuerdo con los procedimientos descritos en este documento.

Todos los módulos que contienen copias de la clave privada de la Entidad de Certificación, en las instalaciones principales o de recuperación del desastre, se encuentran sujetos a este documento.

5. Archivo de la clave privada

Cuando la clave de la Entidad de Certificación de la OMC expira, se archiva durante un periodo de cinco años. Los pares de claves archivados son almacenados de forma segura empleando módulos criptográficos hardware que se encuentran sujetos a lo establecido en este documento, existiendo controles de procedimiento que impiden que la clave archivada sea puesta en producción de nuevo.

Al final del periodo de archivo las claves privadas serán destruidas de forma segura.

La Entidad de Certificación de la OMC no archiva claves privadas de firma electrónica de los usuarios finales.

6. Introducción de la clave privada en el módulo criptográfico

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

7. Almacenamiento de la clave privada en el módulo criptográfico

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

8. Método de activación de la clave privada

La clave privada de la Entidad de Certificación de la OMC se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.B)2.

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

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.

10. Método de destrucción de la clave privada

Las claves privadas son destruidas mediante procedimientos que impiden su robo, modificación, divulgación no autorizada o uso no autorizado, como los procedimientos de ceroización de los propios dispositivos criptográficos.

11. Clasificación de módulos criptográficos

Véase la sección 6.B)1.

C) Otros aspectos de gestión del par de claves

1. Archivo de la clave pública

La Entidad de Certificación de la OMC archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.E) de esta política.

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.

D) Datos de activación

1. Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de la Entidad de Certificación de la OMC son generados de acuerdo con lo establecido en la sección 6.B)2 y los procedimientos de ceremonia de claves. La creación y distribución de dichos dispositivos se registra.

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

2. Protección de datos de activación

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

Los datos de activación de la tarjeta colegial son distribuidos separadamente de la propia tarjeta (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes).

3. Otros aspectos de los datos de activación

Sin estipulación.

E) Controles de seguridad informática

1. Requisitos técnicos específicos de seguridad informática

La Entidad de Certificación de la OMC garantiza que los sistemas que mantienen los programas y datos de la Entidad de Certificación son sistemas seguros que impiden el acceso no autorizado. Adicionalmente, la Entidad de Certificación limita el acceso a los servidores de producción a aquellos individuos que estrictamente resulta necesario. Los usuarios de aplicaciones generales no tienen cuentas en los servidores de producción.

La red de producción de la Entidad de Certificación de la OMC está segregada lógicamente de otros componentes. Esta separación previene el acceso a la red excepto a través de procesos de aplicación definidos. La Entidad de Certificación emplea cortafuegos para proteger la red de producción de intrusiones internas y externas y para limitar la naturaleza y el origen de las actividades de red que pudieran acceder a los sistemas de producción.

La Entidad de Certificación requiere el empleo de contraseñas con una longitud mínima y una combinación de caracteres alfanuméricos y caracteres especiales, debiendo ser cambiada de forma periódica

El acceso directo a las bases de datos de la Entidad de Certificación que ofrece soporte a las operaciones se encuentra limitada a personal fiable.

2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Entidad de Certificación de la OMC son fiables, y han sido certificadas con nivel EAL 4, de

acuerdo con un objetivo de seguridad específico, definido conforme a la norma ISO 15408-3:1999.

F) Controles técnicos del ciclo de vida

1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por la Entidad de Certificación de la OMC de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

2. Controles de gestión de seguridad

La Entidad de Certificación dispone de mecanismos y políticas para controlar y monitorizar la configuración de los sistemas de certificación. La Entidad de Certificación genera resúmenes criptográficos de todos los paquetes de software y de sus actualizaciones.

Este resumen se emplea para verificar la integridad de dicho software manualmente. A partir de la instalación, la Entidad de Certificación valida de forma periódica la integridad de sus sistemas.

3. Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación.

G) Controles de seguridad de red

La Entidad de Certificación de la OMC realiza todas sus operaciones de certificación empleando redes aseguradas, para impedir accesos no autorizados y otras actividades maliciosas. Asimismo, protege las comunicaciones de información sensible mediante el empleo de cifrado y firmas digitales.

H) Controles de ingeniería de módulos criptográficos

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

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

7. Perfiles de certificados y listas de certificados revocados

A) Perfil de certificado

Los certificados tienen el contenido y campos descritos en esta sección, incluyendo, como mínimo, los siguientes:

- Número de serie, que será un código único con respecto al nombre distinguido del emisor
- Algoritmo de firma.
- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 2459
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 2459
- Nombre distinguido del sujeto.
- Clave pública del sujeto, codificada de acuerdo con RFC 2459
- Firma, generada y codificada de acuerdo con RFC 2459

Los certificados son conformes con las siguientes normas:

- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 1999
- ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997
- ETSI TS 101 862 v1.2.1 (2001-06): Qualified Certificate Profile, 2001
- RFC 3039: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, 2001 (siempre que no entre en conflicto con TS 101 862)

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

B) Perfil de la lista de revocación de certificados

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

8. Auditoria de conformidad

VeriSign realiza auditorías de cumplimiento WebTrust sobre su centro de proceso de datos y operaciones de gestión de claves para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios para cumplir la política de los servicios de certificación del Organización Médica Colegial.

1. Frecuencia de la auditoria de conformidad

La auditoría se practica al menos una vez cada año.

2. Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente 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
- Se encuentra acreditada por el American Institute of Certified Public Accountants (AICPA).

3. Relación del auditor con la entidad auditada

Las auditorías de conformidad son realizadas por una firma independiente de VeriSign, sin ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

4. Listado de elementos objeto de auditoria

Los elementos objeto de auditoría serán los siguientes:

- Controles ambientales.
- Operaciones de gestión de claves.
- Controles de infraestructura y administración de la Entidad de Certificación.
- Gestión del ciclo de vida de certificados.
- Divulgación de prácticas de negocio.

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, VeriSign discute, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si se considera que las deficiencias identificadas suponen una amenaza inmediata a la seguridad e integridad de la VeriSign Trust Network, entonces el citado plan será desarrollado en 30 días e implantado en un plazo comercialmente razonable.

6. Tratamiento de los informes de auditoría

Se puede obtener una copia del informe de auditoría WebTrust de VeriSign en la siguiente dirección:

http://www.verisign.com/repository.

9. Requisitos comerciales y legales

A) Tarifas

1. Tarifa de emisión o renovación de certificados

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

2. Tarifa de acceso a certificados

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

3. Tarifa de acceso a información de estado de certificado

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

4. Tarifas de otros servicios

Sin estipulación.

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.

B) Capacidad financiera

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

1. Cobertura de seguro

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

2. Otros activos

Sin estipulación.

3. Cobertura de seguro para suscriptores y terceros que confían en certificados

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

C) Confidencialidad

1. Informaciones confidenciales

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

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

- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

2. Informaciones no confidenciales

La siguiente información se considera no confidencial:

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

3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

4. Divulgación legal de información

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

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

La Entidad de Certificación indicará estas circunstancias en la política de intimidad prevista en la sección 9.D).

5. Divulgación de información por petición de su titular

La Entidad de Certificación de la OMC incluye, en la política de intimidad prevista en la sección 9.D), prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del poseedor de claves, directamente a los mismos o a terceros.

6. Otras circunstancias de divulgación de información

Sin estipulación.

D) Protección de datos personales

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

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

La Entidad de Certificación ha desarrollado una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documentado en su Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad. Esta Declaración de Prácticas de Certificación tiene, por tanto, la consideración de documento de seguridad.

La Entidad de Certificación no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.C)2 a 9.C)6, y en la sección 5.H), en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en este documento, que cumplen las obligaciones previstas en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

E) Derechos de propiedad intelectual

1. Propiedad de los certificados e información de revocación

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

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

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

2. Propiedad de la Declaración de Prácticas de Certificación

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

3. Propiedad de la información relativa a nombres

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

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.A)1.

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.

F) Obligaciones y responsabilidad civil

1. Obligaciones de la Entidad de Certificación de la OMC

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

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

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

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

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

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.E)1, 4.E)2, 9.B), 9.F)7, 9.F)8, 9.F)9 y 9.F)10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público y de la necesidad de empleo de la tarjeta como dispositivo seguro de creación de firma o descifrado de mensajes.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.

- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión de la tarjeta colegial/dispositivo seguro de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.D)2.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

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

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

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.

- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

La Entidad de Certificación, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.D).
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, la Entidad de Certificación garantiza al suscriptor y al tercero que confía en el certificado:

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

3. Rechazo de otras garantías

La Entidad de Certificación de la OMC rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.F)2.

4. Limitación de responsabilidades

La Entidad de Certificación limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores y tarjetas colegiales con la consideración de dispositivo seguro (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por la Entidad de Certificación.

5. Cláusulas de indemnidad

a) Cláusula de indemnidad de suscriptor

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

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

b) Cláusula de indemnidad de tercero que confía en el certificado

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

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

6. Caso fortuito y fuerza mayor

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

7. Ley aplicable

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

8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

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

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.F)1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.C) (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. Cláusula de jurisdicción competente

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

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

10. Resolución de conflictos

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