Servicio de Certificación Digital

Organización Médica Colegial de España

Política de Certificación

Entidad de Certificación de la

Organización Médica Colegial

ÍNDICE

1. Introducción

La sensibilidad de la información sanitaria determina que la necesidad de seguridad es especialmente elevada, tanto por el deber de secreto profesional del profesional médico cuanto por la defensa de las garantías de los pacientes cuya información es tratada.

Las tarjetas inteligentes criptográficas han devenido un elemento esencial en la interacción entre el mundo físico y las nuevas tecnologías, especialmente en la realización de trámites a través de Internet. Gracias a la seguridad que aportan dichas tarjetas, resulta posible desplegar una infraestructura de servicios unificada, en la que se puede ofrecer valor añadido sin renunciar a la necesaria seguridad técnica y jurídica.

Esta afirmación resulta especialmente cierta en el sector de la e-Salud, como se ha reconocido internacionalmente en diversos instrumentos. En concreto, el Plan de Acción eEurope: Una Sociedad de la Información para Todos, inició a principios del año 2000 y en relación con las tarjetas inteligentes, una serie de trabajos – bajo la denominación común de Capítulo de Tarjeta Inteligente (Smart Card Charter) – con especial atención al sector sanitario y, en concreto, a la identificación basada en tarjeta médica.

Dichos trabajos han resultado en un cambio de orientación en relación con el uso de la tarjeta para el sector sanitario, que se configura como el elemento esencial en relación con las infraestructuras de seguridad en la e-Salud, aspecto reconocido de forma preeminente en los más recientes estudios internacionales y, en particular, en el Informe sobre Estrategias en la e-Salud del Comité Europeo de Normalización (2004).

Con la tarjeta médica basada en firma electrónica y certificados reconocidos se puede y se debe aspirar a convertir las redes de acceso e intercambio de información de salud, inseguras en la actualidad, en un elemento transfronterizo completamente seguro de la infraestructura de servicios pan-europeos de e-Salud.

Se convierte, de esta forma, la tarjeta médica en un documento de acceso seguro y fiable a los servicios sanitarios en la red: una llave de acceso que permite la creación de nuevos servicios, como la receta electrónica, la historia clínica compartida, el intercambio de imágenes médicas o el almacenamiento remoto y seguro de información médica, en el pleno respeto de los derechos de los pacientes.

Para ello, sin embargo, se debe exigir el empleo de la firma electrónica reconocida basada en un certificado que acredite la condición de médico colegiado, y producida mediante una tarjeta médica con la condición de dispositivo seguro de creación de firma.

La implantación de la tarjeta de médico no puede ni debe hacerla cualquier entidad, dado que, al representar la tarjeta la condición de colegiado, debe garantizar tanto en el mundo físico como en Internet precisamente que su poseedor es y continua siendo médico. La función de control deontológico y de servicio a la profesión de la tarjeta se debe encontrar fuera de toda duda.

Algunos ejemplos de fraude en entornos sin tarjeta de médico colegiado podrían ser:

- Falsa alegación de ser médico, dado que no se emplea autenticación ni firma electrónica de médico.
- Engaño a la entidad de certificación, por ejemplo con una tarjeta falsa.
- Fraude en el acceso a la información sanitaria, provista por colegios y terceros, incluyendo las administraciones públicas.
- Engaño al paciente respecto a la condición actual de médico colegiado.
- Imposibilidad de detener la actividad o los accesos de un médico expedientado o suspendido.

En definitiva, la tarjeta del colegiado se configura como el elemento clave para la habilitación del colegiado en Internet, que permite que el mismo acceda tanto a los servicios prestados por la Organización Médica Colegial, como por terceros, incluyendo a prestadores de servicios de Internet, administraciones públicas y entidades de certificación, públicas y privadas.

Por todo lo anterior, la Organización Médica Colegial, como entidad legal autorreguladora de la profesión médica, 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.

Los mecanismos de expedición de certificados corporativos por uno o más prestadores de servicios de certificación y los de comprobación de la condición profesional de médico resultan necesarios y compatibles entre sí.
Mientras que los certificados acreditan los datos de identidad personal y la condición de colegiado, como en el caso del servicio prestador por la Entidad de Certificación de la Organización Médica Colegial, resulta necesario en cada transacción re-certificar dicha condición y otras informaciones relativas al colegiado, como garantía corporativa común a todas las aplicaciones sanitarias, públicas y privadas.

Esta política de certificación define los requisitos comunes tanto para la expedición de certificados por la Entidad de Certificación de la Organización Médica Colegial, o por cualquier otro prestador de servicios de certificación corporativos, que debe ser acreditado por la Organización Médica Colegial, como para la validación y, en su caso, re-certificación de la condición corporativa de médico y otras informaciones, para certificados expedidos por cualesquiera prestadores de servicios de certificación, en las diferentes aplicaciones en que resulte necesario.
Todo ello se realiza sobre la base de la tarjeta médica colegial como instrumento de identificación y firma del médico colegiado, así como, en su caso, de otro personal colegial, frente a otros profesionales colegiales, las entidades y corporaciones públicas y privadas, y las Administraciones Públicas.

1.1 Presentación

1.1.1 Modelo de certificación

Este documento describe el modelo de certificación de firma electrónica de la Organización Médica Colegial, que se basa en la tarjeta colegial:

- La Entidad de Certificación de la Organización Médica Colegial es el prestador habitual de servicios de certificación, expidiendo certificados corporativos colegiales, que acreditan la identidad de la persona física y su condición de médico colegiado en ejercicio.
- Pueden, sin embargo, existir otros prestadores de servicios de certificación, que suministren certificados a personas físicas que son profesionales colegiados, incluso sin indicar esta circunstancia, en cuyo caso resulta imprescindible que la Organización Médica Colegial actúe para garantizar la calidad y seguridad de los citados certificados.

Los certificados serán expedidos a entidades finales, incluyendo colegiados, personal administrativo y de servicio, organizaciones y personas físicas que representan a dichas organizaciones, por prestadores de servicios de certificación acreditados por la Organización Médica Colegial.
Los certificados se organizan en clases, atendiendo a los siguientes criterios:

a) Certificados de firma y certificados de cifrado

En cuanto al uso, existen dos tipos de certificados:

1) Certificados de firma electrónica, reconocidos, que se emplean como base de la firma electrónica avanzada, y en conjunción con un dispositivo seguro de creación de firma. También se pueden emplear para firmar mensajes de autenticación (confirmación de la identidad), así como para firmar otros tipos de mensajes.
2) Certificados de cifrado, ordinarios, que se emplean para producir o recibir documentos y mensajes cifrados, de los que se debe guardar copia de la clave privada de descifrado, al objeto de recuperarla en determinadas circunstancias.

b) Certificados corporativos y certificados externos

Los certificados de entidad final pueden ser certificados corporativos o certificados externos:
1) Los certificados corporativos se caracterizan por el hecho de que el suscriptor pertenece a una de las entidades que integran la Organización Médica Colegial. Los certificados corporativos siempre son de colectivo.
2) Los certificados externos son los restantes certificados. Es necesario realizar un registro completo de los datos a certificar.
En general, no se expiden certificados externos, excepto cuando resulte necesario. Los certificados externos pueden ser individuales o de colectivo:

a) Certificados externos individuales, caracterizados por el hecho de que la persona identificada en el certificado actúa en su propio nombre y representación (siendo en este caso el suscriptor o titular del certificado)

b) Certificados corporativos y externos de colectivo, en los que la persona identificada en el certificado actúa en representación y por cuenta de una persona jurídica (que será el suscriptor o titular del certificado).

c) Certificados de colegiado, de órgano colegial y certificados de personal administrativo

Los certificados corporativos pueden expedirse a colegiados o a personal administrativo:
1) Certificados de colegiado, emitidos con la intervención de su Colegio de Médicos, en calidad de registrador con la capacidad exclusiva de certificar la cualidad de “colegiado” de una persona identificada en el certificado.
2) Certificados de órgano colegial de las entidades que integran la Organización Médica Colegial.
3) Certificados de personal administrativo de las entidades que integran la Organización Médica Colegial.

d) Certificados de persona física y certificados de persona jurídica

Los certificados pueden expedirse a personas físicas o a personas jurídicas:
1) Certificados de persona física, que actúa como firmante, debiendo tomarse en cuenta sus apoderamientos y capacidades de actuación, indicadas o no en el certificado, antes de confiar en la firma.
2) Certificados de persona jurídica, a la cual se imputan los documentos firmados, como firmante, sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.

e) Listado de certificados que se pueden expedir
Los prestadores de servicios de certificación podrán expedir, entre otros, los siguientes certificados:
1) Certificado corporativo de colegiado (identificación y firma / cifrado).
2) Certificado corporativo de órgano colegial (identificación y firma / cifrado).
3) Certificado corporativo de personal administrativo (identificación y firma / cifrado).
4) Certificado corporativo de persona jurídica (identificación y firma / cifrado).
5) Certificado externo individual (identificación y firma /cifrado).
6) Certificado externo colectivo (identificación y firma / cifrado).
7) Certificado externo de persona jurídica (identificación y firma / cifrado).

1.1.2 El sistema voluntario de acreditación

La Organización Médica Colegial, en su función de regulación y control de la profesión médica, y con el objeto de garantizar el correcto funcionamiento del sistema de certificación, establece un sistema voluntario de acreditación de la firma electrónica.
El sistema contemplará los siguientes niveles de acreditación:
1) Acreditación de prestadores de servicios de certificación (Colegios y otras entidades, dependiendo del caso).
2) Acreditación (homologación) de tecnologías relacionadas con la firma electrónica.
3) Acreditación (reconocimiento) de jerarquías de certificación.

a) Acreditación de prestadores de servicios de certificación

La acreditación de prestadores de servicios de certificación consiste en el procedimiento por el que la Organización Médica Colegial supervisa la calidad de las operaciones de certificación por parte de un prestador de servicios de certificación, público o privado.

1º Procedimiento de acreditación

Antes de acreditar al prestador de servicios de certificación, se comprobará que el prestador puede demostrar la necesaria fiabilidad de sus servicios.
Todo prestador de servicios de certificación que desee emitir certificados para los usos de la Organización Médica Colegial debe adherirse, al menos, a una política de certificación.
La política de certificado no siempre establece todos los requisitos para un certificado; en mucho casos, se permiten opciones. En ambos casos, partiendo de este documento, el prestador de servicios de certificación puede escribir su propia política de certificado, realizando tales elecciones o concretando los detalles necesarios.
La Organización Médica Colegial analizará la política presentada por el prestador de servicios de certificación, durante el procedimiento de acreditación del prestador, para determinar su conformidad con esta política.
Cada prestador de servicios de certificación debe disponer de una Declaración de Prácticas de Certificación con los procedimientos que aplica en la prestación de sus servicios, como muestra de conformidad con los requisitos establecidos en la política.
Adicionalmente, cada prestador de servicios de certificación debe disponer de la documentación jurídica necesaria para la prestación del servicio, incluyendo los contratos rectores del servicio de certificación.
Todo prestador de servicios de certificación es libre, bajo su plena responsabilidad, de elegir tecnología y jerarquía de certificación. El único requisito que se exige es el cumplimiento de esta política, y la interoperabilidad de los certificados emitidos por cualquier prestador de servicios de certificación mediante el cumplimiento de las instrucciones técnicas de certificación electrónica que dicte la Organización Médica Colegial.

2º Condiciones para la acreditación

La Organización Médica Colegial estudiará el modelo de implantación elegido por el prestador de servicios de certificación y le acreditará, siempre que cumpla los requisitos establecidos en este documento para los tipos de certificados a los que ofrezca soporte, y las siguientes condiciones:

- Que las políticas y procedimientos operados por el prestador de servicios de certificación no son discriminatorios.
- Que el prestador de servicios de certificación ofrecerá sus servicios a todos los solicitantes cuyas actividades entren en el ámbito de operación declarado en su Declaración de Prácticas de Certificación, de acuerdo con lo establecido en la sección 1.3.3 de esta política.

- Que el prestador de servicios de certificación es una entidad legal, de acuerdo con lo establecido en la sección 1.3.1 de esta política.
- Que el prestador de servicios de certificación dispone de sistemas de gestión de la calidad y la seguridad adecuados para la prestación del servicio, dato que será comprobado en la auditoría de conformidad prevista en la sección 8 de esta política.
- Que el prestador de servicios de certificación 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 adecuados de seguridad y de gestión.
- Que el prestador de servicios de certificación cumple los requisitos de capacidad financiera establecidos en la sección 9.2 de esta política.
- Que el prestador de servicios de certificación cumple los requisitos relativos a los procedimientos de resolución de disputas, establecidos en la sección 9.6.10 de esta política.
- Que el prestador de servicios de certificación ha documentado adecuadamente las relaciones jurídicas en virtud de las cuales subcontrata parte o la totalidad de los servicios.
- Que el prestador de servicios de certificación no ha sido condenado por actos dolosos que disminuyan la fiabilidad de los servicios que presta.

3º Excepciones a la acreditación

La Organización Médica Colegial podrá celebrar convenios con entidades públicas prestadoras de servicios de certificación para la colaboración en la expedición de certificados electrónicos, así como con entidades privadas propiedad de entidades públicas, sin necesidad de acreditar a los citados prestadores.

b) Acreditación de tecnologías de firma electrónica

La acreditación de tecnologías de firma electrónica permite agilizar la elección de diferentes tecnologías a los prestadores de servicios de certificación, así como a los usuarios de servicios que emplean la firma electrónica.
La elección de una tecnología acreditada facilita el cumplimiento de los requisitos establecidos en este documento, y acelera el periodo de implantación.
Por otra parte, la acreditación de tecnología permite homologar componentes de generación y verificación de firma, y en particular aplicaciones informáticas que hacen uso de la tarjeta médica colegial.
También incluye la acreditación de tecnologías conexas con los servicios de firma electrónica, como los servicios de sellado de fecha y hora o los servicios de archivo electrónico de documentos firmados.

c) Acreditación de jerarquías de certificación

La acreditación de jerarquías de certificación permite que un prestador de servicios de certificación que forma parte de una jerarquía pueda ser acreditado exitosamente por la Organización Médica Colegial.
Esta política no establece ningún requisito referente a la organización de la jerarquía; en general, el requisito para acreditar una jerarquía es la compatibilidad y adaptabilidad de la misma a los requisitos establecidos en esta política.

d) Convenios rectores

La Organización Médica Colegial establecerá los convenios rectores necesarios con las diferentes entidades acreditadas.

1.1.3 Los servicios de validación e información

La Organización Médica Colegial prestará servicios de validación e información en relación con los certificados expedidos de acuerdo con esta política.
Dichos servicios consisten en la comprobación en tiempo real de la condición de médico colegiado y otras informaciones corporativas de que disponga en cada momento la Organización Médica Colegial, como garantía complementaria a la ofrecida por el certificado expedido al profesional médico almacenado en su tarjeta médica.

1.2 Nombre del documento e identificación

Este documento es la “Política de Certificación de la Organización Médica Colegial”.
La Declaración de Prácticas de Certificación de la Organización Médica Colegial debe asignar a cada tipo de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.
Cada prestador de servicios de certificación podrá establecer libremente sus identificadores de objeto.

1.3 Participantes en los servicios de certificación

Esta política de certificación establece una comunidad de usuarios, que obtienen certificados para diversos usos y aplicaciones profesionales relacionadas con las entidades que integran la Organización Médica Colegial, así como otras entidades relacionadas con el ejercicio de la profesión.

Los prestadores de servicios de certificación adheridos a esta política general de certificación no expiden los certificados corporativos al público, ni siquiera cuando se trata de certificados reconocidos, como el certificado de firma de colegiado.
Los prestadores de servicios de certificación podrán expedir otros certificados, como los certificados externos, al público.

1.3.1 Prestadores 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.

a) Organización Médica Colegial

El papel de la Organización Médica Colegial es garantizar la calidad en el empleo de los medios electrónicos, informáticos y telemáticos por los profesionales médicos y, por tanto, debe acreditar a los prestadores de servicios de certificación, de acuerdo con las políticas de certificación establecidas en este documento.

b) Prestador de servicios de certificación

El papel de los prestadores de servicios de certificación es la emisión y gestión de claves y certificados de entidad final, incluyendo personas, dentro y fuera del ámbito corporativo, y organizaciones.
Puede ser las siguientes entidades:
1) La propia Organización Médica Colegial, a través de la Entidad de Certificación que constituya al efecto.
2) Otras organizaciones, públicas y privadas, que deberán ser acreditadas por el Organización Médica Colegial.

1.3.2 Registradores

En general, los registradores de certificados corporativos son las entidades de la Organización Médica Colegial, y en especial, los Colegios de Médicos.
La Organización Medica Colegial dispondrá de un Sistema Unificado de Registro (SUR) de los diferentes Colegios, y asistirá técnicamente en el registro a los Colegios de Médicos que lo soliciten.

Los prestadores de servicios de certificación podrán disponer los registradores, públicos o privados, que consideren oportuno, para certificados externos.

1.3.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para firma, autenticación y cifrado.
Serán entidades finales del sistema de certificación de la Organización Médica Colegial las siguientes entidades:
1) Solicitantes de certificados.
2) Suscriptores de certificados.
3) Poseedores de claves.
4) Terceros que confían en certificados.

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) La persona que va a ser el futuro suscriptor del certificado, típicamente el Colegio correspondiente.
2) Una persona autorizada por el futuro suscriptor.
3) Una persona autorizada por el registrador, cuando el registrador sea diferente al suscriptor.
4) Una persona autorizada por el prestador de servicios de certificación.

b) Suscriptores de certificados

Los suscriptores son las personas y las organizaciones identificadas en el certificado, en especial los Colegios correspondientes.
El suscriptor tiene licencia de uso del certificado, y, cuando se trata de una organización, otorga el uso del certificado a 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, en su caso, de descifrado.
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 de descifrado, a diferencia de la clave de firma del certificado de firma electrónica, puede ser recuperada, en ciertos casos y condiciones, por el prestador de servicios de certificación.
Para que la clave de descifrado se pueda recuperar, resulta obligatorio que sea una clave diferente de la clave de firma, por ejemplo, mediante la emisión de certificados de clave pública diferentes.

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 este documento de política y en los documentos jurídicos correspondientes.

1.3.4 Otros participantes

a) Proveedores técnicos

Los proveedores técnicos son entidades públicas y privadas dedicadas al suministro de:
1) Los componentes informáticos, incluyendo aplicaciones informáticas y bienes de equipo, necesarios para la prestación de servicios de certificación.
2) Servicios de certificación en régimen de prestación externa, llave en mano y otras modalidades análogas.

b) Jerarquías externas de certificación

Las jerarquías externas de certificación son formas preestablecidas de organización de prestadores de servicios de certificación, que frecuentemente ofrecen servicios de valor añadido, dentro de los cuales puede incardinarse una Entidad de Certificación que presta servicios.

1.4 Uso de los certificados

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

1.4.1 Usos permitidos para los certificados

a) Certificado de firma

Los certificados de firma electrónica son certificados reconocidos, de acuerdo con lo establecido en el artículo 6 de la Ley 59/2003, de 19 de diciembre, en caso de certificados de personas físicas, y de acuerdo con el artículo 7 de la misma Ley, en caso de certificados de personas jurídicas, con el contenido prescrito por el artículo 11 de la Ley 59/2003, y expedidos siguiendo las prescripciones de los artículos 12, 13 y 17 a 21 de la propia Ley.

Los certificados de firma electrónica corresponden a certificados reconocidos con dispositivo seguro de creación de firma electrónica, no expedidos al público cuando son corporativos, de acuerdo con la especificación técnica TS 101 456 v1.4.1, del Instituto Europeo de Normas de Telecomunicaciones.

Los certificados de firma electrónica deben emplearse necesariamente con un dispositivo seguro de creación de firma electrónica, que cumpla los requisitos establecidos por el artículo 24 de la Ley 59/2003 y esta política.

Garantizan la identidad del suscriptor y del poseedor de la clave privada de firma, resultando idóneos para ofrecer soporte a la firma electrónica reconocida; esto es, la firma electrónica avanzada que se basa en certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo que, de acuerdo con el artículo 3 de la Ley 59/2003, se equipara a la firma manuscrita por efecto legal, sin necesidad de cumplir requisito adicional alguno.

b) Certificado de cifrado

Los certificados de cifrado son, como mínimo, certificados ordinarios, y garantizan la identidad del suscriptor y, en su caso, del poseedor de la clave de cifrado; asimismo, deben emplearse en conjunción con un dispositivo de generación de protección de la clave privada de descifrado razonablemente seguro.

Los certificados de cifrado siguen la norma técnica TS 102 042 v1.2.1, del Instituto Europeo de Normas de Telecomunicaciones.

Permiten el cifrado y descifrado de mensajes y documentos por parte del poseedor de claves. La clave privada del certificado de cifrado podrá ser archivada de forma que, en ciertas circunstancias, pueda recuperarse y acceder a la información cifrada, incluso sin la

intervención del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos o de colectivo.

1.4.2 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.
Los certificados de firma electrónica no pueden emplearse para firmar mensajes de autenticación incomprensibles para el firmante, en particular desafíos de cliente SSL o TLS, y tampoco se pueden emplear para recibir mensajes cifrados.

1.5 Administración de la política

1.5.1 Organización que administra el documento

Esta política es administrada por la Organización Médica Colegial de España.

1.5.2 Datos de contacto de la organización

Los datos de contacto de la Organización Médica Colegial de España son los siguientes:
Plaza de las Cortes, 11- 28014 Madrid.
Teléfono: 91 431 77 80. Fax: 91 576 43 88.

1.5.3 Procedimientos de gestión del documento

Este documento se aprobará de acuerdo con el procedimiento que se determine al efecto.

2. Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

Cada prestador de servicios de certificación deberá disponer de un Depósito de certificados.
El servicio de Depósito estará disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control del prestador de servicios de certificación, éste realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 y la Declaración de Prácticas de Certificación aplicable.
El prestador de servicios de certificación podrá delegar esta obligación en la Organización Médica Colegial o, en su caso, en el correspondiente Consejo Autonómico. En todo caso, dichas entidades deberán valorar la posibilidad de asumir dicha obligación.

2.2 Publicación de información del prestador de servicios de certificación

El prestador de servicios de certificación publicará las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento del poseedor de claves
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados, o su adherencia a esta política de certificación.
- La Declaración de Prácticas de Certificación.
- Los documentos jurídicos vinculantes con suscriptores y terceros que confían en certificados.

2.3 Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo políticas y la Declaración de Prácticas de Certificación, se publicará en cuanto se encuentre disponible.
Los cambios en los documentos de política y en la Declaración de Prácticas de Certificación se regirán por lo establecido en la sección 1.5 del documento de política o Declaración de Prácticas de Certificación.
La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en las secciones 4.6.6 y 4.6.7 de esta política.

2.4 Control de acceso

El prestador de servicios de certificación no limitará el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establecerá controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información de estado de revocación.
El prestador de servicios de certificación empleará 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

3.1 Gestión de nombres

3.1.1 Tipos de nombres

Todos los certificados contendrán un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=).

a) Certificados corporativos

El prestador de servicios de certificación podrá emplear el esquema de nombres que considere más apropiado, siempre que cumpla con las siguientes condiciones:

- Debe incluir el nombre del Registrador: por ejemplo, el Colegio de Médicos al que pertenezca el suscriptor o la entidad en la que preste sus servicios el personal administrativo.
- Debe incluir el número de colegiado del poseedor de la clave y el Documento Nacional de Identidad, o equivalente, del colegiado o del personal administrativo.
- Debe ser un formato de nombres aceptado por las Administraciones Públicas y, en especial, por la Administración Tributaria.

b) Certificados externos

El prestador de servicios de certificación podrá emplear el esquema de nombres que considere más apropiado, siempre que cumpla con las siguientes condiciones:

- Debe ser un formato de nombres aceptado por las Administraciones Públicas y, en especial, por la Administración Tributaria.
- En certificados corporativos y externos de colectivo, debe indicarse el nombre de la organización a la que se encuentra vinculado el poseedor de claves.

c) Certificados de persona jurídica

El prestador de servicios de certificación podrá emplear el esquema de nombres que considere más apropiado, siempre que cumpla con las siguientes condiciones:

- Debe ser un formato de nombres aceptado por las Administraciones Públicas y, en especial, por la Administración Tributaria.

- Debe incluir el Documento Nacional de Identidad, o equivalente, del responsable de la custodia de los datos de creación de firma electrónica correspondientes a los datos de verificación de firma contenidos en el certificado de persona jurídica.
- Debe incluir el Código de Identificación Fiscal de la persona jurídica suscriptora del certificado.

3.1.2 Significado de los nombres

Los nombres de los certificados serán interpretados de acuerdo con la legislación española aplicable a los nombres de las personas físicas y jurídicas.

3.2 Empleo de anónimos y seudónimos

En ningún caso se pueden emplear anónimos ni seudónimos.

3.2.1 Interpretación de formatos de nombres

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

3.2.2 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada servicio de generación de certificados operado por un prestador de servicios de certificación.
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.

3.2.3 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.
El prestador de servicios de certificación no estará obligado 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.

a) Certificados corporativos

En los certificados corporativos, además del número del Documento Nacional de Identidad, o equivalente, se podrá incluir el número de colegiado o de personal administrativo, cuando éstos existan.

b) Certificados externos

En certificados externos individuales, los conflictos de nombres de suscriptores que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado del certificado, del número de Documento Nacional de Identidad, o equivalente, del suscriptor.
En certificados corporativos y externos de colectivo, los conflictos de nombres de poseedores de claves que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado del certificado, del número del Documento Nacional de Identidad, o equivalente, del poseedor de la clave, así como del número del Código de Identificación Fiscal de la persona jurídica.

3.2.4 Tratamiento de marcas registradas

Véase la sección 3.2.3.

3.3 Validación inicial de la identidad

En esta sección se establecen requisitos relativos a los procedimientos de identificación y autenticación que deben emplearse durante el registro de suscriptores, incluyendo colectivos y personas físicas, que debe realizarse con anterioridad a la emisión y entrega de certificados.
Los requisitos de validación de la identidad son diferentes en certificados corporativos y en certificados externos.
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 – médicos colegiados y personal administrativo – se puede validar con 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 deben ser inscritos en la Agencia correspondiente de Protección de Datos, por la Organización Médica Colegial.
Por el contrario, la identidad de los suscriptores y poseedores de claves de los certificados externos, debe ser validada de forma completa, dado que no existen registros corporativos válidos a emplear.

3.3.1 Prueba de posesión de clave privada

Esta sección describe los métodos a emplear para demostrar que se posee la clave privada correspondiente a la clave pública objeto de certificación.

El método de demostración de posesión de la clave privada será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método fiable aprobado por la Organización Médica Colegial.
Este requisito no se aplica cuando el par de claves es generado por el registrador, por delegación del suscriptor, durante el proceso de personalización 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.

3.3.2 Autenticación de la identidad de una organización

Esta sección contiene requisitos para la comprobación de la identidad de una organización identificada en el certificado o que interviene en procesos de certificación digital.

a) Registradores externos

El prestador de servicios de certificación debe autenticar, con carácter previo a la emisión y entrega de un certificado de operador perteneciente a un registrador externo, diferente de una entidad que integra la Organización Médica Colegial, la identidad del registrador y del operador del registro, de acuerdo con lo establecido en la sección 3.1.1.b para certificados corporativos y externos de colectivo.
Para ello, el prestador de servicios de certificación podrá emplear los siguientes métodos:

1) Obtención de información acerca de la organización, de un proveedor externo de servicios de esta naturaleza.
2) Comprobación de documentación justificativa aportada por el solicitante. En este caso, se requerirá la presencia física o equivalente del representante del futuro registrador.

b) Suscriptores de certificados

1º Certificados corporativos

No se requiere realizar procedimiento de autenticación de la organización titular del certificado en certificados corporativos (Colegio o Consejo), dado que la organización forma parte del ámbito corporativo de la Organización Médica Colegial.

2º Certificados externos

El prestador de servicios de certificación debe autenticar, con carácter previo a la emisión y entrega de un certificado externo de colectivo, la identidad del suscriptor y otros datos, de acuerdo con lo establecido en la sección 3.1.1.b para certificados corporativos y externos de colectivo.
El prestador de servicios de certificación podrá emplear registradores, propios o externos, para esta tarea.
Para ello, el prestador de servicios de certificación o el registrador podrán emplear los siguientes métodos:
1) Obtención de información acerca de la organización, de un proveedor externo de servicios de esta naturaleza, a discreción del prestador de servicios de certificación, que previamente deberá aprobar al proveedor externo.
2) Comprobación de documentación justificativa aportada por el solicitante, acerca de los siguientes extremos:

a) Nombre legal completo de la organización.
b) Estado legal de la organización.
c) Número de identificación fiscal.
d) Datos de identificación registral.

3.3.3 Autenticación de la identidad de una persona física

Esta sección contiene requisitos para la comprobación de la identidad de una persona física identificada en un certificado o que interviene en procesos de certificación digital.

a) Elementos de identificación requeridos

El prestador de servicios de certificación establecerá el número y los tipos de documentos que sean necesarios para acreditar la identidad del poseedor de la clave, pudiendo emplear los siguientes:
1) Documento Nacional de Identidad.
2) Número de Identificación de Extranjero.

b) Validación de los elementos de identificación

1º Certificados corporativos

Los registros colegiales, que serán integrados en el Sistema de Registro Unificado (SUR), son los únicos que legalmente permiten acreditar la condición de colegiado o personal administrativo.
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 internos del registrador, que debe asegurarse de la corrección de la información a certificar.

2º Certificados externos

La información de identificación de suscriptores de certificados externos individuales, así como de poseedores de claves de certificados corporativos y externos de colectivo, se realiza contrastando la información de la solicitud con la documentación aportada, electrónicamente o en soporte físico.
También es posible emplear procedimientos notariales de identificación y autenticación, a discreción del prestador de servicios de certificación.

c) 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, el prestador de servicios de certificación deberá contrastar la identidad del suscriptor de certificados externos individuales o del poseedor de claves de certificados corporativos y externos de colectivo mediante la presencia física directa o indirecta del mismo.

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

d) Vinculación de la persona física con una organización

1º Certificados corporativos

Dado que se trata de certificados corporativos, no es preciso obtener una justificación documental adicional de la vinculación del poseedor de la clave con la entidad integrada en la Organización Médica Colegial.

2º Certificados externos

Cuando se expidan certificados corporativos y externos de colectivo, el prestador de servicios de certificación debe obtener una justificación documental de la vinculación de la persona física con la organización, mediante cualquier medio admitido en derecho.
El prestador de servicios de certificación podrá emplear registradores externos para esta tarea.

3.3.4 Información de suscriptor no verificada

No se podrá incluir información de suscriptor no verificada en los certificados.

3.4 Identificación y autenticación de solicitudes de renovación

3.4.1 Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el prestador de servicios de certificación deberá comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.
Si cualquier información del suscriptor o del poseedor de la clave hubiere cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección 3.3.

3.4.2 Validación para la renovación de certificados tras la revocación

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado – siempre y cuando la causa de la revocación hubiese sido diferente del compromiso de la clave privada – el prestador de servicios de certificación deberá comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.
Si cualquier información del suscriptor o del poseedor de la clave hubiere cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección 3.3.

3.5 Identificación y autenticación de la solicitud de revocación

El prestador de servicios de certificación deberá autenticar las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.
Dichas peticiones e informes serán confirmados cumpliendo los procedimientos establecidos en la Declaración de Prácticas de Certificación del prestador de servicios de certificación.

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

4.1 Solicitud de emisión de certificado

4.1.1 Legitimación para solicitar la emisión

Antes de la emisión y entrega de un certificado, debe existir una solicitud de certificado, de oficio o a instancia de parte interesada.
En caso de que solicitante y suscriptor sean entidades diferentes, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumentará jurídicamente.

4.1.2 Procedimiento de alta; Responsabilidades

Podrán existir los siguientes tipos de solicitudes:
1) Certificados corporativos. Solicitud electrónica de certificado de oficio (no contiene clave pública, ni se encuentra firmada digitalmente).
2) Certificados corporativos/externos. Solicitud electrónica de certificado de parte sin generación de claves (no contiene clave pública, ni se encuentra firmada digitalmente).
3) Certificados corporativos/externos. Solicitud electrónica de certificado de parte con generación de claves (PKCS#10 o mecanismo compatible, con la clave pública del usuario y su firma digital, al objeto de demostrar la posesión de la clave privada, de acuerdo con la sección 3.3.1 de la presente política de certificado).

a) Certificados corporativos

El prestador de servicios de certificación deberá recibir solicitudes de certificados, realizadas de oficio por las entidades que integran la Organización Médica Colegial, o a instancia de los colegiados.
En este caso debe existir un documento, ya sea en soporte papel o en formato electrónico, referente a la petición de certificados, realizada por la organización al prestador de servicios 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.

b) Certificados externos

El prestador de servicios de certificación deberá recibir solicitudes de certificados realizadas por el futuro suscriptor, en cuyo caso pueden concurrir diversas circunstancias:

- Existe un documento, ya sea en papel o en formato electrónico, de la petición del certificado.
- El solicitante genera su par de claves o acepta expresamente que se le generarán y librarán en el correspondiente dispositivo seguro.
- Cuando el solicitante ha generado su par de claves, debe enviar la clave pública para certificación y demostrar que posee la clave privada (de acuerdo con lo establecido en la sección 3.3.1 de esta política de certificación).
- El solicitante acepta un acuerdo de suscriptor, acuerdo que pueden ser unas condiciones generales de emisión.

c) Certificados de firma electrónica

El prestador de servicios de certificación debe asegurarse de que las solicitudes de certificado son completas, precisas y están debidamente autorizadas.
Antes de la emisión y entrega del certificado, el prestador de servicios de certificación informará al suscriptor, en caso de certificados externos individuales, o al poseedor de claves, en caso de certificados corporativos y externos de colectivo, de los términos y condiciones aplicables al certificado.
La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible.
A la solicitud se deberá acompañar documentación justificativa de la identidad del suscriptor y otras circunstancias, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, de acuerdo con lo establecido en la sección 3.3.3 de esta política de certificados.
También se deberá acompañar una dirección física, u otros datos, que permitan contactar al suscriptor, en caso de certificados externos individuales, o al poseedor de claves, en caso de certificados corporativos y externos de colectivo.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, el prestador de servicios de certificación debe verificar la información proporcionada, conforme a la sección 3.3 de esta política.

4.2.2 Aprobación o rechazo de la solicitud

Si la verificación no es correcta, o si se sospecha que no es correcta, el prestador de servicios de certificación debe denegar la petición, o detener su aprobación hasta haber realizado las comprobaciones oportunas.
En caso de que los datos se verifiquen correctamente, el prestador de servicios de certificación deberá aprobar la solicitud del certificado.
El prestador de servicios de certificación deberá notificar al solicitante la aprobación o denegación de la solicitud.

4.2.3 Plazo para resolver la solicitud

Cada prestador de servicios de certificación podrá establecer el plazo que considere oportuno para resolver las solicitudes de certificados, plazo de que deberá ser aprobado previamente por la Organización Médica Colegial.

4.3 Emisión del certificado

4.3.1 Acciones del prestador de servicios de certificación durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procederá a la emisión del certificado y grabación en la tarjeta, de forma segura y se pondrá la misma a disposición del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, para su aceptación, de acuerdo con lo establecido en la sección 4.3.2.
Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

a) Procedimiento general

El prestador de servicios de certificación deberá:

- Emplear un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- En caso de que el prestador de servicios de certificación genere el par de claves, emplear un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves, y que la clave privada es almacenada de forma segura en la tarjeta del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

- Proteger la confidencialidad e integridad de los datos de registro, especialmente en caso de que sea intercambiados con el suscriptor, en caso de certificados externos individuales, con el poseedor de claves, en caso de certificados de corporativos y externos de colectivo o con el tercer solicitante, en su caso.

b) Condiciones adicionales para el certificado de firma electrónica

Cuando emita certificados de firma electrónica, el prestador de servicios de certificación también deberá:

- Incluir en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de 19 de diciembre, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1 de esta política.
- Indicar la fecha y la hora en que se expidió un certificado.
- En los casos en que el prestador de servicios de certificación aporta el dispositivo seguro de creación de firma, emplear un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al suscriptor, en caso de certificados externos individuales, o al poseedor de claves, en caso de certificados corporativos y externos de colectivo.
- Utilizar 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.
- Asegurarse de que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso de que el prestador de servicios de certificación genere claves privadas, que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.

4.3.2 Notificación de la emisión al suscriptor

El prestador de servicios de certificación notificará la emisión del certificado al suscriptor o, en su caso, poseedor de claves; que el certificado se encuentra disponible y el modo de obtenerlo.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades del prestador de servicios de certificación

El prestador de servicios de certificación deberá:

- Si no lo ha hecho antes, acreditar definitivamente la identidad del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, de acuerdo con lo establecido en las secciones 3.3.2 y 3.3.3 de esta política.

- Proporcionar al suscriptor, en caso de certificados externos individuales, o al futuro poseedor de claves, en caso de certificados corporativos y externos de colectivo, acceso al certificado.
- Entregar, en su caso, el dispositivo criptográfico de firma, verificación de firma, cifrado o descifrado.
- En caso de certificados corporativos y externos de colectivo, entregar al poseedor de claves una hoja de libramiento del certificado (y, en su caso, del dispositivo criptográfico mencionado en el apartado anterior), 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 del dispositivo criptográfico.
  c) Reconocimiento por parte del poseedor, de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de los citados elementos.
  d) Obligaciones del poseedor de claves.
  e) Responsabilidad del poseedor de claves.
  f) Método de imputación exclusiva al poseedor de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones 6.2 y 6.4 de esta política.
  g) La fecha del acto de entrega y aceptación.

4.4.2 Conducta que constituye aceptación del certificado

El prestador de servicios de certificación documentará en su Declaración de Prácticas de Certificación y en su documentación jurídica, la(s) conducta(s) que constituya(n) aceptación del certificado, conducta que en general podrá consistir en la firma de la hoja de entrega del certificado.

4.4.3 Publicación del certificado

El prestador de servicios de certificación publicará el certificado en el Depósito a que se refiere la sección 2.1 de esta política, con los controles de acceso pertinentes.

4.4.4 Notificación de la emisión a terceros

El prestador de servicios de certificación, excepto en el caso de la Entidad de Certificación de la Organización Médica Colegial, notificará en todo caso la emisión de los certificados a dicha Organización Médica Colegial.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el suscriptor

a) Obligaciones del suscriptor del certificado

1º Régimen general

El prestador de servicios de certificación obligará al suscriptor a:

- Facilitar al prestador de servicios de certificación información completa y adecuada, conforme a los requerimientos de esta política de certificado, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Cumplir las obligaciones que se establecen para el suscriptor en la presente política de certificación.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4 de esta política.
- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la presente política de certificación.
- Comunicar al prestador de servicios 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 del dispositivo seguro de creación de firma) o por cualquier otra causa.
  c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2 de esta política.
- Transferir a los poseedores de claves las obligaciones específicas de los mismos.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación del prestador de servicios de certificación ni de la Organización Médica Colegial, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación del prestador de servicios de certificación ni de la Organización Médica Colegial, sin permiso previo por escrito.

2º Condiciones adicionales para el certificado de firma electrónica

Cuando emita certificados de firma electrónica, el prestador de servicios de certificación también obligará al suscriptor a:

- Emplear el par de claves exclusivamente para firmas electrónicas y conforme a cualesquiera otras limitaciones que le sean notificadas.
- Ser especialmente diligente en la custodia de su clave privada y de su dispositivo seguro de creación de firma, con el fin de evitar usos no autorizados.
- En caso que el suscriptor genere sus propias claves, se le deberá obligar a:
  a) Generar sus claves de suscriptor empleando un algoritmo reconocido como aceptable para la firma electrónica reconocida.
  b) Crear las claves dentro del dispositivo seguro de creación de firma
  c) Emplear longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.
- Notificar al prestador de servicios de certificación, sin retrasos injustificables, la pérdida, la alteración, el uso no autorizado, el robo o el compromiso de su dispositivo seguro de creación de firma.

El suscriptor del certificado de firma electrónica que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado, deberá reconocer, en el debido documento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, conforme a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre.

b) Responsabilidad civil del suscriptor de certificado

1º Garantías ofrecidas por el suscriptor

El prestador de servicios de certificación deberá obligar al suscriptor, mediante el correspondiente documento jurídico, a garantizar:

- En caso de que el suscriptor fuese el solicitante del certificado, 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 del prestador de servicios de certificación.
- Que cada firma digital creada empleando la clave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.
- 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.

- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del suscriptor.

2º Protección de la clave privada

El prestador de servicios de certificación deberá obligar al suscriptor, mediante el correspondiente documento jurídico, a garantizar que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

4.5.2 Uso por el tercero que confía en certificados

a) Obligaciones del tercero que confía en certificados

1º Régimen general

El prestador de servicios de certificación debe obligar 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
- 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 del prestador de servicios de certificación ni de la Organización Médica Colegial, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación del prestador de servicios de certificación ni de la Organización Médica Colegial, sin permiso previo por escrito.

2º Certificado de firma electrónica

El tercero que confía en un certificado de firma electrónica deberá reconocer, en el debido documento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con el artículo 3 de la Ley 59/2003, de 19 de diciembre.

b) Responsabilidad civil del tercero que confía en certificados

El prestador de servicios de certificación deberá obligar al tercero que confía en el certificado, mediante el correspondiente documento jurídico, a manifestar:

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

4.6 Revocación y suspensión de certificados

El prestador de servicios de certificación deberá detallar en su Declaración de Prácticas de Certificación los siguientes aspectos:

- Quién puede solicitar la revocación.
- Cómo se remitirá la solicitud.
- Los requisitos de confirmación de solicitudes de revocación.
- Si se pueden suspender certificados, y las causas de suspensión.
- Los mecanismos empleados para distribuir información de estado de revocación.
- El máximo retraso entre la recepción de la solicitud y la disponibilidad por terceros que confían en certificados del cambio del estado de revocación, que no podrá superar en ningún caso el plazo de un día.

4.6.1 Causas de revocación de certificados

Un prestador de servicios de certificación podrá revocar un certificado debido, por lo menos, a 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.

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 el prestador de servicios de certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la Declaración de Prácticas de Certificación del prestador de servicios de certificación.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

d) Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

e) El uso irregular del certificado por el suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, o falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan a la seguridad del dispositivo criptográfico:

a) Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.

b) Pérdida o inutilización por daños del dispositivo criptográfico.

c) Acceso no autorizado, por un tercero, a los datos de activación del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

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

a) Finalización de la relación jurídica entre el prestador de servicios de certificación y el suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

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

d) Infracción por el suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente o en la Declaración de Prácticas de Certificación del prestador de servicios de certificación que le emitió el certificado.

e) La incapacidad sobrevenida o el fallecimiento del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.

f) En caso de certificados corporativos y externos de colectivo, 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 3.5 de esta política.

5) Otras circunstancias:

a) La suspensión del certificado digital por un período superior al establecido en la sección 4.6.14 de esta política.

b) La terminación del servicio del prestador de servicios de certificación, de acuerdo con lo establecido en la sección 5.8 de esta política.

El prestador de servicios de certificación podrá establecer otras causas de revocación, siempre que resulten compatibles con el ordenamiento jurídico y, en concreto, con la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Asimismo, deberá adaptar las causas anteriores a cada caso concreto; por ejemplo, indicando las causas por las que un médico colegiado puede dejar de serlo, siendo, por tanto, necesario revocar su certificado.

Si la entidad a la que se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión.

En este caso se considerará que las actuaciones realizadas durante el período de suspensión no son válidas, siempre y cuando el certificado finalmente sea revocado. Serán válidas si se levanta la suspensión y el certificado vuelve a pasar a la situación de válido.

El documento jurídico que vincula al prestador de servicios de certificación con el suscriptor establecerá que el suscriptor deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

4.6.2 Legitimación para solicitar la revocación

Podrán solicitar la revocación de un certificado:

- En caso de certificados externos individuales, el suscriptor a nombre del cual el certificado fue emitido.
- En caso de certificados corporativos y externos de colectivo, un representante autorizado por el suscriptor, o el propio poseedor de claves.
- El registrador que solicitó la emisión del certificado, o cualquier otro que reciba una solicitud de revocación.

4.6.3 Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo al prestador de servicios de certificación o, en su caso, al 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 al prestador de servicios de certificación o, en su caso, al registrador que proceda.
La solicitud debe ser autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 3.5 de esta política, antes de proceder a la revocación.
En caso de que el destinatario de la solicitud fuera el registrador, una vez autenticada, podrá revocar directamente el certificado o remitir una solicitud en este sentido al prestador de servicios de certificación.
La solicitud de certificación será procesada a su recepción.
Se deberá informar al suscriptor y, en su caso, al poseedor de claves, acerca del cambio de estado del certificado revocado.
El prestador de servicios de certificación no podrá reactivar el certificado, una vez revocado.

4.6.4 Plazo temporal de solicitud de revocación

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

4.6.5 Obligación de consulta de información de revocación de certificados

Los terceros que confían en certificados 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 el prestador de servicios de certificación que emitió el certificado en el cual se desea confiar.
El prestador de servicios de certificación deberá suministrar información a los terceros que confían en certificados acerca de cómo y dónde encontrar la Lista de Revocación de Certificados correspondiente.

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

El prestador de servicios de certificación deberá emitir una LRC al menos cada 24 horas.
Se deberá indicar en la LRC el momento programado de emisión de una nueva LRC, si bien se podrá emitir una LRC antes del plazo indicado en la LRC anterior.
Los certificados revocados que expiren serán retirados de la LRC transcurridos sesenta días desde la expiración.

4.6.7 Disponibilidad de servicios de comprobación de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados del Prestador de servicios de certificación, que deberá estar disponible las 24 horas de los 7 días de la semana.
En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control del prestador de servicios de certificación, éste deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantiene inactivo el mínimo tiempo posible.
El prestador de servicios de certificación detallará en su Declaración de Prácticas de Certificación el periodo máximo de tiempo en el que el servicio deberá volver a operar.
El prestador de servicios de certificación deberá suministrar información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

4.6.8 Obligación de consulta de servicios de comprobación de estado de certificados

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

4.6.9 Otras formas de información de revocación de certificados

El prestador de servicios de certificación podrá implantar otras formas de provisión de información acerca del estado de revocación de los certificados, debiendo describir las provisiones correspondientes a su funcionamiento en su Declaración de Prácticas de Certificación.

4.6.10 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de un prestador de servicios de certificación será notificado, en la medida de lo posible, a todos los participantes en los servicios de certificación del Organización Médica Colegial.
El prestador de servicios de certificación detallará en su Declaración de Prácticas de Certificación el modo en que dará cumplimiento a esta obligación.

4.6.11 Causas de suspensión de certificados

El prestador de servicios de certificación podrá suspender un certificado si sospecha el compromiso de una clave, hasta que éste sea confirmado.
El prestador de servicios de certificación debe asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.6.12 Legitimación para solicitar la suspensión

Podrán solicitar la suspensión de un certificado:

- En caso de certificados externos individuales, el suscriptor a nombre del cual el certificado fue emitido.
- En caso de certificados corporativos y externos de colectivo, un representante autorizado por el suscriptor, o propio el poseedor de claves.
- El registrador que solicitó la emisión del certificado, o cualquier otro que reciba una solicitud de suspensión.

4.6.13 Procedimientos de petición de suspensión

Para proceder a una solicitud electrónica de suspensión, el suscriptor o, en su caso el poseedor de claves, deberá disponer de un certificado válido, para autenticarse frente al prestador de servicios de certificación o, en su caso, a un registrador.
Si no dispone de certificado, se dirigirá a un prestador de servicios de certificación o, en su caso, a un registrador para instar la suspensión.
El prestador de servicios de certificación debe determinar en su Declaración de Prácticas de Certificación los procedimientos y mecanismos de acceso a los sistemas de suspensión.

4.6.14 Plazo máximo de suspensión

El plazo máximo de suspensión será de treinta días naturales.

4.7 Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.
Como excepción, el suscriptor podrá mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determine esta política y la Declaración de Prácticas de Certificación del prestador.

En el caso de los certificados corporativos, el prestador de servicios de certificación podrá emitir de oficio un nuevo certificado de colegiado o de personal administrativo, mientras los suscriptores mantengan dicho estado.

4.8 Depósito y recuperación de claves

4.8.1 Política y prácticas de depósito y recuperación de claves

El prestador de servicios de certificación podrá mantener un depósito de claves privadas de descifrado, siempre que lo haga de forma segura, dividiendo las claves o el acceso a las mismas en al menos dos partes, que deberán encontrarse bajo la custodia de personas o entidades diferentes.
Las claves sólo se podrán recuperar en las siguientes circunstancias:

- A petición del poseedor de la clave, o de sus herederos o tutor, en caso de incapacitación.
- A petición del suscriptor (titular de la clave), o de su entidad sucesora, cuando resulte procedente.
- En caso de investigación civil o criminal, mediante petición del Juez competente.

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

Sin estipulación.

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

5.1 Controles de seguridad física

El prestador de servicios de certificación debe disponer de instalaciones que protejan físicamente la prestación de, al menos, los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.
La protección física se logrará mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones debe encontrarse fuera de estos perímetros.
El prestador de servicios de certificación establecerá 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 deberá establecer prescripciones para las siguientes contingencias, que se documentarán sucintamente en la Declaración de Prácticas de Certificación del prestador:

- 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.

5.1.1 Localización y construcción de las instalaciones

La localización de las instalaciones debe permitir la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos (en el caso de no contar con presencia física permanente de personal de seguridad del prestador de servicios de certificación)

La calidad y solidez de los materiales de construcción de las instalaciones deberá garantizar unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

5.1.2 Acceso físico

El prestador de servicios de certificación deberá establecer niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.
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, serán imprescindibles las siguientes medidas cuando dichos procesos sean realizados por empresas subcontratadas por la Entidad de Certificación de la OMC: 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 reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.
Cuando dichos procesos sean realizados por entidades u organizaciones dependientes de la Organización Médica Colegial serán imprescindibles la autorización previa y la identificación en el momento del acceso y registro del mismo.
La generación de claves criptográficas de los prestadores de servicios de certificación, así como su almacenamiento, deberá realizarse en dependencias específicas para estos fines, y requerirán de acceso y permanencia duales.

5.1.3 Electricidad y aire acondicionado

Los equipos informáticos del prestador de servicios de certificación deberán estar convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.
Las instalaciones contarán 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 requiera el cierre ordenado y completo de todos los sistemas informáticos.
Los equipos informáticos deberán estar ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

5.1.4 Exposición al agua

El prestador de servicios de certificación deberá disponer 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.

5.1.5 Prevención y protección de incendios

Todas las instalaciones y activos del prestador de servicios de certificación deben contar con sistemas automáticos de detección y extinción de incendios.
En concreto, los dispositivos criptográficos, y soportes que almacenen claves de los prestadores de servicios de certificación, deberán contar con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

5.1.6 Almacenamiento de soportes

El almacenamiento de soportes de información debe realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.
Deberá contarse para ellos con dependencias o armarios ignífugos.
El acceso a estos soportes, incluso para su eliminación, deberá estar restringido a personas específicamente autorizadas.

5.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se deberá realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.
En el caso de soportes magnéticos, se procederá al formateo, borrado permanente, o destrucción física del soporte.
En el caso de documentación en papel, éste deberá someterse a un tratamiento físico de destrucción.

5.1.8 Copia de respaldo fuera de las instalaciones

Periódicamente, el prestador de servicios de certificación almacenará copia de respaldo de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

5.2 Controles de procedimientos

Los prestadores de servicios de certificación deben garantizar que sus sistemas se operan de forma segura, para lo cual deberá establecer e implantar procedimientos para las funciones que afecten a la provisión de sus servicios.
El personal al servicio del prestador de servicios de certificación realizará los procedimientos administrativos y de gestión de acuerdo con la política de seguridad del prestador de servicios de certificación.

5.2.1 Funciones fiables

El prestador de servicios de certificación deberá identificar, en su política de seguridad, funciones o roles con la condición de fiables.
Las personas que deban ocupar tales puestos deberán ser formalmente nombrados por la alta dirección del prestador de servicios de certificación.
Las funciones fiables deberán incluir:

- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Auditores del sistema.

5.2.2 Número de personas por tarea

Las funciones fiables identificadas en la política de seguridad del prestador de servicios de certificación, y sus responsabilidades asociadas, serán documentadas en descripciones de puestos de trabajo, y descritas de forma sucinta en la Declaración de Prácticas de Certificación del prestador.
Dichas descripciones deberán realizarse teniendo en cuenta que debe existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.
Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

5.2.3 Identificación y autenticación para cada función

El prestador de servicios de certificación deberá identificar y autenticar al personal antes de acceder a la correspondiente función fiable.

5.2.4 Roles que requieren separación de tareas

Las siguientes tareas deberán ser realizadas, al menos, por dos personas:

- Gestión del acceso físico.
- Gestión de aplicaciones informáticas del prestador.

- Gestión de configuración y control de cambios.
- Gestión del archivo.
- Gestión de bienes de equipo criptográfico.
- Generación de certificados de autoridad de certificación.

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

El prestador de servicios de certificación deberá emplear 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 aplicará al personal de gestión del prestador de servicios de certificación, especialmente en relación con procedimientos de personal de seguridad.
La calificación y la experiencia podrán suplirse mediante una formación y entrenamiento apropiados.
El personal en puestos fiables deberá encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.
El prestador de servicios de certificación no podrá 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, el prestador de servicios de certificación deberá realizar una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a los siguientes aspectos:

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

5.3.2 Procedimientos de investigación de historial

El prestador de servicios de certificación deberá realizar la investigación antes de que la persona sea contratada y acceda al puesto de trabajo.
En la solicitud para el puesto de trabajo se informará acerca de la necesidad de someterse a una investigación previa.
Se deberá advertir de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.
El prestador de servicios de certificación deberá obtener consentimiento inequívoco del afectado por la investigación previa y procesar y proteger todos sus datos personales de

acuerdo con la LOPD y REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.La investigación se repetirá cada tres años.

5.3.3 Requisitos de formación

El prestador de servicios de certificación deberá formar al personal en puestos fiables y de gestión, hasta que alcancen la cualificación necesaria, de acuerdo con lo establecido en la sección 5.3.1 de esta política.
La formación deberá incluir los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Versiones de maquinaria y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.

5.3.4 Requisitos y frecuencia de actualización formativa

El prestador de servicios de certificación deberá realizar una actualización en la formación del personal al menos cada dos años.

5.3.5 Secuencia y frecuencia de rotación laboral

El prestador de servicios de certificación podrá establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

5.3.6 Sanciones para acciones no autorizadas

El prestador de servicios de certificación deberá disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que deberá encontrarse 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 podrán incluir la suspensión y el despido de la persona responsable de la acción dañina.

5.3.7 Requisitos de contratación de profesionales

El prestador de servicios de certificación podrá contratar profesionales para cualquier función, incluso para un puesto fiable, en cuyo caso deberá someterse a los mismos controles que los restantes empleados.
En el caso de que el profesional no deba someterse a tales controles, deberá estar constantemente acompañado por un empleado fiable, cuando se encuentre en las instalaciones del prestador de servicios de certificación.

5.3.8 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 que sea suficientemente competente a tenor de lo establecido en la sección 5.3.1 de esta política.

5.4 Procedimientos de auditoria de seguridad

5.4.1 Tipos de eventos registrados

El prestador de servicios de certificación debe guardar registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas.
- Inicio y terminación de la aplicación de autoridad de certificación o de autoridad de registro central.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves del prestador de servicios de certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red del prestador de servicios de certificación.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el Depósito de certificados.
- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

El prestador de servicios de certificación debe también guardar, ya sea manual o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Los registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo.
- Posesión de datos de activación, para operaciones con la clave privada del prestador de servicios de certificación.

5.4.2 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.
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 también deben ser documentadas.

5.4.3 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 5.5.2 de esta política.

5.4.4 Protección de los registros de auditoría

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

5.4.5 Procedimientos de copia de respaldo

Se deberán generar, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

5.4.6 Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría deberá ser, al menos, un sistema interno del prestador de servicios de certificación, 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 serán almacenados por el personal debidamente autorizado.

5.4.7 Notificación del evento de auditoria al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.
Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8 Análisis de vulnerabilidades

Los eventos en el proceso de auditoría deberán ser guardados, en parte, para monitorizar las vulnerabilidades del sistema.
Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.
Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, del prestador de servicios de certificación.

5.5 Archivo de informaciones

El prestador de servicios de certificación debe garantizar que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1 Tipos de eventos registrados

El prestador de servicios de certificación debe guardar todos los eventos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación del mismo.
El prestador de servicios de certificación debe guardar un registro de lo siguiente:

- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- Identidad del Registrador que acepta la solicitud de certificado.

- La ubicación de las copias de solicitudes de certificados y del documento firmado por el suscriptor, en caso de certificados externos individuales, o del poseedor de las claves, en caso de certificados corporativos y externos de colectivo.

5.5.2 Periodo de conservación de registros

El prestador de servicios de certificación debe guardar los registros especificados en la sección anterior de esta política durante 15 años.

5.5.3 Protección del archivo

El prestador de servicios de certificación debe:

- Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archivar los datos anteriormente citados de forma completa y confidencial.
- Mantener la privacidad de los datos de registro del suscriptor, en caso de certificados externos individuales, o del poseedor de las claves, en caso de certificados corporativos y externos de colectivo.

5.5.4 Procedimientos de copia de respaldo

El prestador de servicios de certificación debe realizar copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección 5.5.1 de esta política. Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta política.
Además, el prestador de servicios de certificación debe guardar los documentos en papel, según la sección 5.5.1, en un lugar fuera de las instalaciones de la propia prestador de servicios de certificación para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta política.

5.5.5 Requisitos de sellado de fecha y hora

El prestador de servicios de certificación debe emitir los certificados y las LRCs con información fiable de fecha y hora.
No es necesario que esta información se encuentre firmada digitalmente.

5.5.6 Localización del sistema de archivo

El prestador de servicios de certificación debe disponer de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, tal y como se especifica en la sección 5.5.4 de esta política.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Sólo personas autorizadas por el prestador de servicios de certificación podrán tener acceso a los datos de archivo, ya sea en las mismas instalaciones del prestador de servicios de certificación o en su ubicación externa.

5.6 Renovación de claves

Cuando se solicite la renovación de un par de claves, el registrador debe verificar que los datos de registro siguen siendo válidos y, si algún dato ha cambiado este debe ser verificado, guardado y el suscriptor debe estar de acuerdo con él, tal y como se especifica en la sección 4.1 de esta política.

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos el prestador de servicios de certificación debe iniciar las gestiones necesarias, de acuerdo con el plan de seguridad, el plan de emergencia y el plan de auditoría, o documentos que los sustituyan, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.2 Revocación de la clave pública de la entidad

La Organización Médica Colegial podrá exigir a un prestador de servicios de certificación perteneciente a una jerarquía acreditada que revoque la clave pública de un prestador de servicios de certificación acreditado.
En el caso de que un prestador de servicios de certificación perteneciente a una jerarquía acreditada deba revocar la clave pública de un prestador de servicios de certificación acreditado, deberá llevar a cabo lo siguiente:

- Notificar este hecho, cuando se produzca, a la Organización Médica Colegial.
- Informar del hecho publicando una LRC, según lo establecido en la sección 4.6.6 de esta política.
- Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales el prestador de servicios de certificación Acreditado emitió certificados así como a los terceros que confían en certificados que deseen confiar en esos certificados.
- Realizar una renovación de claves, en caso de que la revocación no haya sido debida a la terminación del servicio por parte del prestador de servicios de certificación acreditado, según lo establecido en la sección 5.6 de esta política.

5.7.3 Compromiso de la clave privada de la entidad

El plan de continuidad de negocio del prestador de servicios de certificación (o plan de recuperación de desastres) debe considerar el compromiso o la sospecha de compromiso de la clave privada del prestador de servicios de certificación como un desastre.

En caso de compromiso, el prestador de servicios de certificación debe proporcionar como mínimo lo siguiente:

- Informar a todos los suscriptores y verificación del compromiso.
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de este prestador de servicios de certificación ya no son válidos.

5.7.4 Desastre sobre las instalaciones

El prestador de servicios de certificación debe desarrollar, mantener, probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indique cómo restaurar los servicios de los sistemas de información.
La ubicación de los sistemas de recuperación de desastres debe disponer de las protecciones físicas de seguridad detalladas en el plan de seguridad.
El prestador de servicios de certificación debe ser capaz de restaurar la operación normal de los servicios de suspensión y, en su caso, de revocación, en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Suspensión de certificados.
- En su caso, revocación de certificados.
- Publicación de información de revocación.

La base de datos de recuperación de desastres utilizada por el prestador de servicios de certificación debe estar 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 del prestador de servicios de certificación deben tener las medidas de seguridad físicas especificadas en el plan de seguridad.

5.8 Terminación del servicio

El prestador de servicios de certificación debe asegurar 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.

Antes de terminar sus servicios, el prestador de servicios de certificación debe ejecutar, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y terceros que confían en certificados.
- Retirar toda autorización de subcontrataciones que actúan en nombre del prestador de servicios de certificación en el proceso de emisión de certificados.
- Ejecutar 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.
- Destruir las claves privadas del prestador de servicios de certificación o retirarlas del uso.

El prestador de servicios de certificación debe declarar en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas deben incluir:

- Notificación a las entidades afectadas.
- Transferencia de las obligaciones del prestador de servicios de certificación a otras partes.
- Cómo se tratará el estado de revocación de los certificados emitidos que aún no han expirado.

6. Controles de seguridad técnica

El prestador de servicios de certificación deberá emplear sistemas y productos fiables, que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El prestador de servicios de certificación que actúe como raíz de una jerarquía acreditada procederá a la generación de las claves de prestador de servicios de certificación de acuerdo con la ceremonia de claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.
Cuando el prestador de servicios de certificación no forme parte de ninguna jerarquía acreditada, generará y firmará su propio par de claves, de acuerdo con la ceremonia de claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.
Los pares de claves de los prestadores de servicios de certificación (tanto el prestador de servicios de certificación raíz de la jerarquía acreditada como los prestadores de servicios de certificación acreditados) deben ser generados empleando hardware criptográfico que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 partes 1 a 4, según proceda; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.
Los pares de claves de los suscriptores y de los operadores y administradores de las registradores, deberán generarse siempre en dispositivos criptográficos que cumplan ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14167 partes 1 a 4, según proceda; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.

6.1.2 Envío de la clave privada al suscriptor

La clave privada del suscriptor, en certificados externos individuales, o al poseedor de claves, en certificados corporativos y externos de colectivo, deberá serle entregada debidamente protegida mediante una tarjeta inteligente que cumpla lo establecido en ISO 15408: EAL 4 + (o superior), de acuerdo con lo establecido en CEN CWA 14169 o criterios de seguridad equivalentes.
En caso de certificados de médico, se entregarán única y exclusivamente en la tarjeta de médico colegiado, expedida por la Organización Médica Colegial, con independencia de cuál sea el prestador de servicios de certificación que expida el certificado.

6.1.3 Envío de la clave pública al emisor del certificado

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

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

Las claves de prestadores de servicios de certificación deben ser comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen.
La clave pública del prestador de servicios de certificación raíz de una jerarquía acreditada se publicará en el Depósito, en forma de certificado autofirmado, junto a una declaración referente a que la clave autentica al prestador de servicios de certificación.
Cuando el prestador de servicios de certificación no forme parte de ninguna jerarquía acreditada, publicará su propio certificado autofirmado en el Depósito.
Se deberán establecer medidas adicionales para confiar en el certificado autofirmado, como la comprobación de la huella digital del certificado.
Los usuarios podrán acceder al Depósito para obtener las claves públicas del prestador de servicios de certificación.
Adicionalmente, en aplicaciones S/MIME, el mensaje de datos podrá contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

6.1.5 Tamaños de claves

La longitud de las claves de los prestadores de servicios de certificación será al menos de 2048 bits, mientras que la de los restantes tipos de certificados será de al menos 1024 bits.

6.1.6 Generación de parámetros de clave pública

Sin estipulación.

6.1.7 Comprobación de calidad de parámetros de clave pública

La Organización Médica Colegial podrá establecer métodos de comprobación de la calidad de los parámetros de las claves públicas.

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

Las claves de los prestadores de servicios de certificación se generarán en hardware criptográfico que cumpla el estándar ISO 15408: EAL 4 (o superior), de acuerdo con lo

dispuesto en CEN CWA 14167, parte 3, o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.
Las claves de firma electrónica de los usuarios finales se generarán en tarjetas inteligentes que cumplan el estándar ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en CEN CWA 14169, o criterios de seguridad equivalentes.
La generación de claves para los restantes tipos de certificados podrá realizarse mediante aplicaciones informáticas.

6.1.9 Propósitos de uso de claves

El prestador de servicios de certificación podrá incluir la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

6.2 Protección de la clave privada

6.2.1 Estándares de módulos criptográficos

Para los módulos que gestionan claves de los prestadores de servicios de certificación y de los suscriptores de certificados de firma electrónica, se deberá asegurar el nivel exigido por los estándares indicados en las secciones anteriores.

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

El acceso a las claves privadas de los prestadores de servicios de certificación, deberá requerir necesariamente del concurso simultáneo de tres (3) dispositivos criptográficos protegidos por una clave de acceso, de entre cinco (5) dispositivos.
La clave de acceso será conocida únicamente por una persona responsable de ese dispositivo. Ninguna de ellas conocerá más que una de las claves de acceso.
Los dispositivos criptográficos quedarán almacenados en las dependencias del prestador de servicios de certificación, y para su acceso será necesaria una persona adicional.

6.2.3 Depósito de la clave privada

Las claves privadas de los prestadores de servicios de certificación se almacenarán en espacios ignífugos y protegidos por controles de acceso físico dual.
Las claves privadas de los certificados no se podrán almacenar en el prestador de servicios de certificación, excepto en caso de certificados exclusivos de cifrado, como se establece en la sección 4.8.1 de esta política.

6.2.4 Copia de respaldo de la clave privada

La clave privada del prestador de servicios de certificación deberá contar con una copia de respaldo realizada, almacenada en dependencia independiente de aquélla donde se almacena habitualmente, y recuperada en su caso, por personal sujeto a la política de confianza del personal. Este personal debe ser expresamente autorizado a estos fines, y debe limitarse a aquel que necesite hacerlo en las prácticas del prestador de servicios de certificación.
Los controles de seguridad a aplicar a las copias de respaldo del prestador de servicios de certificación deberán ser de igual o superior nivel a los que se aplican a las claves habitualmente en uso.
Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

6.2.5 Archivo de la clave privada

No se archivarán claves privadas de firma electrónica de usuarios finales.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se podrán generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.
Las claves privadas de los prestadores de servicios de certificación quedarán almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes (de las que no podrán ser extraídas)
Dichas tarjetas serán empleadas para introducir la clave privada en el módulo criptográfico.

6.2.7 Método de activación de la clave privada

La clave privada del prestador de servicios de certificación se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.
La clave privada del suscriptor se activará mediante la introducción del PIN en la tarjeta inteligente.

6.2.8 Método de desactivación de la clave privada

Para certificados personales, cuando la tarjeta inteligente se retire del dispositivo lector, o la aplicación que la utilice finalice la sesión, será necesaria nuevamente la introducción del PIN.

6.2.9 Método de destrucción de la clave privada

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

El prestador de servicios de certificación podrá archivar sus claves públicas, de acuerdo con lo establecido en la sección 5.5 de esta política.

6.3.2 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves serán los determinados por la duración del certificado, transcurrido el cual no podrán continuar utilizándose.
Como excepción, la clave privada de descifrado podrá continuar empleándose incluso tras la expiración del certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Si el prestador de servicios de certificación facilita al suscriptor un dispositivo seguro de creación de firma, entonces los datos de activación del dispositivo, deberán ser generados de forma segura por el prestador de servicios de certificación.

6.4.2 Protección de datos de activación

Cuando el prestador de servicios de certificación facilite al suscriptor el dispositivo seguro de creación de firma, como es la tarjeta de médico colegiado, los datos de activación del dispositivo, deberán ser distribuidos separadamente del propio dispositivo de creación de firma (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes)
Como excepción, cuando el suscriptor, en caso de certificados externos individuales, o el poseedor de claves, en caso de certificados corporativos y externos de colectivo, reciba presencialmente su certificado, en un dispositivo, de un registrador, deberá seleccionar e introducir los datos de activación, de modo que únicamente los conozca él.

6.4.3 Otros aspectos de los datos de activación

Sin estipulación.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de seguridad informática

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados. En particular:

- El prestador de servicios de certificación debe garantizar una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.
- El prestador de servicios de certificación debe garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas del prestador, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado.
- El personal del personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal del prestador será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma)
- El acceso a los depósitos públicos de la información del prestador (por ejemplo, certificados o información de estado de revocación) deberá contar con un control de accesos para modificaciones o borrado de datos.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por el prestador de servicios de certificación deberán ser fiables, por ejemplo de acuerdo con un perfil de protección adecuado, conforme a la norma ISO 15408 o equivalente.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de autoridad de certificación y de registro, para garantizar que los sistemas son seguros.
Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

6.6.2 Controles de gestión de seguridad

El prestador de servicios de certificación deberá mantener un inventario de todos los activos informativos y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.
La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección 0 de esta política.
Se realizará un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

6.6.3 Evaluación del nivel de seguridad del ciclo de vida

La Organización Médica Colegial podrá exigir que el prestador de servicios de certificación se someta a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos del prestador.

6.7 Controles de seguridad de red

Se deberá garantizar que el acceso a las diferentes redes del prestador de servicios de certificación está limitado a individuos debidamente autorizados. En particular:

- Deben implementarse controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos deberán configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación del prestador de servicios de certificación.
- Los datos sensibles deberán protegerse cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
- Se debe garantizar que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.8 Controles de ingeniería de módulos criptográficos

Se debe garantizar que las claves de los prestadores de servicios de certificación son generadas en dispositivos criptográficos, operados por personal de confianza de la Entidad y en un entorno seguro bajo control dual.

Estos dispositivos deben cumplir los estándares criptográficos de seguridad, que se han indicado en las secciones anteriores.

Los algoritmos de generación de claves deberán estar aceptados para el uso de la clave a que esté destinado (para los diferentes tipos de certificados que se definen).

7. Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Los certificados tendrán 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 serán 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

Adicionalmente, los certificados de firma electrónica serán conformes con las siguientes normas:

- 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 Organización Médica Colegial publicará sus perfiles de certificados y se reserva el derecho a supervisar el contenido de los perfiles de certificados expedidos por los prestadores de servicios de certificación, y proponer los cambios que resulten necesarios para garantizar su funcionamiento interoperable con la tarjeta de médico colegiado.

7.2 Perfil de la lista de revocación de certificados

La Organización Médica Colegial publicará sus perfiles de listas de revocación y se reserva el derecho a supervisar el contenido de los perfiles de las listas de revocación de certificados expedidas por los prestadores de servicios de certificación, y proponer los cambios que resulten necesarios para garantizar su funcionamiento interoperable con los servicios de información ofrecidos por las entidades que integran la Organización Médica Colegial.

8. Auditoria de conformidad

El prestador de servicios de certificación debe realizar periódicamente una auditoría de cumplimiento 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.
Además de la auditoría de conformidad, el prestador de servicios de certificación debe estar preparado para pasar otras revisiones, no periódicas, que demuestren su fiabilidad:

- Antes de acreditar un nuevo prestador de servicios de certificación, debe realizársele una revisión de sus documentos de seguridad y Declaración de Prácticas de Certificación para asegurar que cumple con los requisitos de seguridad y de operación necesarios, como se establece en la sección 1.1.2.a de esta política.
- Si se sospecha que, en cualquier momento, el prestador de servicios de certificación no cumple con alguno de los requisitos de seguridad o si se ha detectado un compromiso de claves, ya sea una sospecha o real, o cualquier evento que pueda suponer un peligro para la seguridad o integridad del prestador de servicios de certificación, se llevará a cabo una auditoría interna.

8.1 Frecuencia de la auditoria de conformidad

El prestador de servicios de certificación debe llevar a cabo una auditoría de conformidad anualmente, además de las auditorías internas que pueda llevar a cabo bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.2 Identificación y calificación del auditor

Si el prestador de servicios de certificación dispone de un departamento de auditoría interno, éste podrá encargarse de llevar a cabo la auditoría de conformidad.
En el caso de no poseer ese departamento, el prestador de servicios de certificación deberá acudir a un auditor independiente, el cual debe demostrar experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública.

8.3 Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros deben ser llevadas a cabo por una entidad independiente del prestador de servicios de certificación auditada, la cual no debe tener ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

8.4 Listado de elementos objeto de auditoria

Los elementos objeto de auditoría serán los siguientes:

- Procesos de certificación de clave pública.
- Sistemas de información.
- Protección del centro de proceso
- Documentación del servicio.

Los detalles de cómo llevar a cabo la auditoría de cada uno de estos elementos se detallarán en el plan de auditoría del prestador de servicios de certificación.

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, el prestador de servicios de certificación debe discutir, con la entidad que ha ejecutado la auditoría y con la Organización Médica Colegial, las deficiencias encontradas y desarrollar y ejecutar un plan correctivo que solvente dichas deficiencias.

Si el prestador de servicios de certificación auditado es incapaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá realizarse una de las siguientes acciones:

- Revocar la clave del prestador de servicios de certificación, tal y como se describe en la sección 5.7.2 de esta política.
- Terminar el servicio del prestador de servicios de certificación, tal y como se describe en la sección 5.8 de esta política.

8.6 Tratamiento de los informes de auditoría

El prestador de servicios de certificación debe entregar los informes de resultados de auditoría, a la Organización Médica Colegial, en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

El prestador de servicios de certificación podrá establecer una tarifa por la emisión o por la renovación de los certificados, que deberá ser comunicada a la Organización Médica Colegial.

9.1.2 Tarifa de acceso a certificados

El prestador de servicios de certificación no podrá establecer ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

El prestador de servicios de certificación no podrá establecer ninguna tarifa por el acceso a la información de estado de los certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación.

9.1.5 Política de reintegro

El prestador de servicios de certificación debe disponer de una política de reintegro de la tarifa, que deberá documentar en su Declaración de Prácticas de Certificación.

9.2 Capacidad financiera

El prestador de servicios de certificación deberá disponer de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios.

9.2.1 Cobertura de seguro

El prestador de servicios de certificación deberá disponer de una garantía de cobertura de su responsabilidad civil suficiente, bien mediante un seguro de responsabilidad civil profesional por errores y omisiones, bien mediante una fianza o aval.
La cuantía garantizada deberá ser de 3.000.000 euros o superior.

9.2.2 Otros activos

Sin estipulación.

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

Sin estipulación.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones serán mantenidas confidenciales por el prestador de servicios de certificación:

- 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 el prestador de servicios de certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

9.3.2 Informaciones no confidenciales

La siguiente información será considerada no confidencial, y de esta forma será reconocido por los afectados, en el documento jurídico vinculante con el prestador de servicios de certificación:

- Los certificados emitidos o en trámite de emisión.

- La vinculación del suscriptor a un certificado emitido por el prestador de servicios de certificación.
- El nombre y los apellidos del suscriptor del certificado, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, así como cualesquiera 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 suscriptor del certificado, en caso de certificados externos individuales, o del poseedor de claves, en caso de certificados corporativos y externos de colectivo, 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 de esta política.

9.3.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

El prestador de servicios de certificación divulgará 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 serán 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.
El prestador de servicios de certificación indicará estas circunstancias en la política de intimidad prevista en la sección 9.4 de esta política.

9.3.5 Divulgación de información por petición de su titular

El prestador de servicios de certificación incluirá, en la política de intimidad prevista en la sección 9.4 de esta política, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del poseedor de claves, directamente a los mismos o a terceros.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de datos personales

Para la prestación del servicio, el prestador de servicios de certificación precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones serán recabadas directamente de los afectados, con su consentimiento explícito o en los casos es los que la ley permita recabar la información sin consentimiento del afectado.
El prestador de servicios de certificación recabará los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.
El prestador de servicios de certificación deberá desarrollar una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documentar 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. Dicha Declaración de Prácticas de Certificación tendrá la consideración de documento de seguridad.
El prestador de servicios de certificación no divulgará ni cederá datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6 de esta política, y en la sección 5.8, en caso de terminación del prestador de servicios de certificación.
La información confidencial de acuerdo con la LOPD será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas 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.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

El prestador de servicios de certificación será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita.
El prestador de servicios de certificación deberá conceder 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 aplicación de esta política, según se

define en la sección 1.4, y de acuerdo con el correspondiente instrumento vinculante entre el prestador de servicios de certificación y la parte que reproduzca y/o distribuya el certificado
Las anteriores reglas figurarán en los instrumentos vinculantes entre el prestador de servicios de certificación y los suscriptores y los terceros que confían en certificados.
Adicionalmente, los certificados emitidos por el prestador de servicios de certificación deben contener un aviso legal relativo a la propiedad de los mismos.
Las mismas reglas resultarán de aplicación al uso de información de revocación de certificados.

9.5.2 Propiedad de la política de certificado y Declaración de Prácticas de Certificación

El Organización Médica Colegial será la única entidad que gozará de los derechos de propiedad intelectual sobre las políticas de certificados del Organización Médica Colegial.
Cada prestador de servicios de certificación será propietario de su Declaración de Prácticas de Certificación.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, el poseedor de claves, conservará cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.
El suscriptor será el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 de esta política.

9.5.4 Propiedad de claves

Los pares de claves serán propiedad de los suscriptores de los certificados.
Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave serán propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Modelo de obligaciones del prestador de servicios de certificación

El prestador de servicios de certificación debe garantizar, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política de certificado para la que emite certificados.

El prestador de servicios de certificación será la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

El prestador de servicios de certificación debe prestar sus servicios de certificación conforme con su Declaración de Prácticas de Certificación vigente, en la que se detallarán sus funciones, procedimientos de operación y medidas de seguridad.

Antes de la emisión y entrega del certificado al suscriptor, el prestador de servicios de certificación deberá informarle de los términos y condiciones relativos al uso del certificado, de su precio – cuando se establezca – y de sus limitaciones de uso.

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

El prestador de servicios de certificación debe vincular a suscriptores, poseedores de claves y terceros que confían en certificados mediante documentos jurídicos apropiados, especificados en su Declaración de Prácticas de Certificación.

Estos documentos jurídicos deberán estar en lenguaje escrito y comprensible, y debe tener los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.2, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10 de la presente política de certificación.
- Indicación de la política aplicable, con indicación de sí los certificados se expiden al público y de la necesidad de empleo de 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 del dispositivo seguro de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones del prestador de servicios de certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2 de esta política.
- 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 del prestador de servicios de certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales el prestador de servicios 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 el prestador de servicios de certificación ha sido declarado conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

El prestador de servicios de certificación debe asumir otras obligaciones incorporadas directamente en el certificado o incorporadas por referencia.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

El prestador de servicios de certificación, en los documentos jurídicos que le vinculen con suscriptores y terceros que confían en certificados, establecerá y rechazará garantías, y establecerá limitaciones de responsabilidad aplicables.
El prestador de servicios de certificación, como mínimo, garantizará al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por el prestador de servicios de certificación y, en su caso, por el registrador.
- 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.

El prestador de servicios de certificación, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4 de la presente política de certificación.
- 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, cuando emita un certificado de firma electrónica, el prestador de servicios de certificación garantizará 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 del prestador de servicios de certificación, con los límites que se establezcan.

9.6.3 Rechazo de otras garantías

El prestador de servicios de certificación podrá rechazar toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4 Limitación de responsabilidades

El prestador de servicios de certificación limitará su responsabilidad a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por el prestador de servicios de certificación.
El prestador de servicios de certificación podrá limitar su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede emplearse el certificado.

9.6.5 Cláusulas de indemnidad

a) Cláusula de indemnidad de suscriptor

El prestador de servicios de certificación deberá incluir, en el documento jurídico que le vincule con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne al prestador de servicios 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 al prestador de servicios de certificación, el Registrador o 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

El prestador de servicios de certificación deberá incluir, en el documento jurídico que le vincule con el tercero que confía en el certificado, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne al prestador de servicios de certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

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

9.6.6 Caso fortuito y fuerza mayor

El prestador de servicios de certificación incluirá cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en los documentos jurídicos con los que vincule a suscriptores y terceros que confían en certificados.

9.6.7 Ley aplicable

El prestador de servicios de certificación deberá establecer, en sus documentos jurídicos vinculantes con suscriptores y terceros que confían en certificados, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

9.6.8 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

El prestador de servicios de certificación deberá establecer, en sus documentos jurídicos vinculantes con suscriptores y terceros que confían en certificados, 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, el prestador de servicios de certificación velará porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación de la política de certificación y de los documentos jurídicos que vinculen al prestador de servicios de certificación con suscriptores y terceros que confían en certificados.

- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9 Cláusula de jurisdicción competente

El prestador de servicios de certificación deberá establecer, en sus documentos jurídicos vinculantes con suscriptores y terceros que confían en certificados, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.
La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10 Resolución de conflictos

El prestador de servicios de certificación deberá establecer, en sus documentos jurídicos vinculantes con suscriptores y terceros que confían en certificados, los procedimientos de mediación y resolución de conflictos aplicables.
Las situaciones de discrepancia que se deriven de la utilización del empleo de los certificados emitidos por el prestador de servicios de certificación, se resolverán aplicando los mismos criterios de competencia que en los casos de los documentos firmados manuscritamente.
En los supuestos de controversia producidos como consecuencia de la gestión de los certificados entre las diferentes entidades o personas físicas que integran la organización de la infraestructura de clave pública del prestador de servicios de certificación, se estará a lo establecido en la Declaración de Prácticas de Certificación aplicable.