

POLÍTICA Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS

CERTIFICADOS DE COMPONENTE

“AC COMPONENTES INFORMÁTICOS”

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / v1.8	20/02/2019
Revisado por:	FNMT-RCM / v1.8	4/03/2019
Aprobado por:	FNMT-RCM / v1.8	5/03/2019

HISTÓRICO DEL DOCUMENTO – CONTROL DE CAMBIOS			
Versión	Fecha	Descripción	Autor
(1.0)	21/11/2013	Primera versión	FNMT-RCM
(1.1)	07/03/2014	Eliminación de la Suspensión	FNMT-RCM
(1.2)	22/10/2014	Revisión conforme WebTrust	FNMT-RCM
(1.3)	23/03/2015	Inclusión del OID del certificado para uso de Unidades de Sellado de Tiempo	FNMT-RCM
(1.4)	24/06/2016	Eliminación de componentes de personas físicas y actualización de perfiles: inclusión de campo Locality...	FNMT-RCM
(1.5)	03/01/2017	Adaptación al reglamento eIDAS	FNMT-RCM
(1.6)	09/10/2017	Incorporación de requisitos CAB/Forum	FNMT-RCM
(1.7)	21/09/2018	Incorporación de requisitos CAB/Forum	FNMT-RCM
(1.8)	5/03/2019	Incorporación de requisitos CAB/Forum en materia de validación de dominios.	FNMT-RCM

Referencia: DPC/PC-DPC-ACCOMP-0108/SGPSC/2019

Documento clasificado como: *Público*

Índice de contenidos

1. Introducción.....	4
2. Organización del documento	5
3. Definiciones	6
4. Orden de prelación.....	7
5. Política de certificación de los certificados de componente	7
5.1. Identificación.....	7
5.2. Seudónimos.....	9
5.3. Reconocimiento y autenticación de marcas registradas	9
5.4. Comunidad y ámbito de aplicación	9
5.4.1. Participantes.....	10
5.5. Responsabilidades y obligaciones de las partes	10
5.5.1. Responsabilidades de las partes	10
5.5.1.1. Responsabilidad del Prestador de Servicios de Confianza	11
5.5.1.2. Responsabilidad del Solicitante	12
5.5.1.3. Responsabilidad del Suscriptor	12
5.5.1.4. Responsabilidad de la Entidad Usuaria y terceros que confían	13
5.5.2. Obligaciones y garantías de las partes	13
5.5.2.1. Obligaciones y Garantías del Prestador de Servicios de Confianza	13
5.5.2.2. Obligaciones de la Oficina de Registro	15
5.5.2.3. Obligaciones del Solicitante y Suscriptor.....	16
5.5.2.4. Obligaciones de la Entidad Usuaria y terceros que confían	17
5.6. Límites de uso de los certificados y aceptación del mismo.....	17
6. Prácticas de certificación particulares para los certificados de componente “AC Componentes Informáticos”	18
6.1. Gestión del ciclo de vida de los Certificados de Componente.....	18
6.1.1. Procedimiento de solicitud.....	18
6.1.2. Suscripción y envío del contrato por el Suscriptor	19
6.1.3. Validación del dominio	19
6.1.4. Expedición	20
6.1.5. Publicación y distribución.....	21
6.1.6. Notificación al solicitante	21
6.1.7. Vigencia.....	21
6.1.7.1. Caducidad.....	21
6.1.7.2. Extinción de la vigencia del Certificado.....	22
6.1.8. Renovación	22
6.1.9. Revocación	22
6.1.9.1. Causas de revocación	23
6.1.9.2. Procedimiento para la revocación de Certificados	24
6.1.9.3. Efectos y periodo de la revocación.....	25

6.1.10.	Suspensión	25
6.1.11.	Información del cambio de estado del Certificado	25
6.1.12.	Comprobación del estado del Certificado	25
6.2.	<i>Certificado de componente para el servicio FNMT de Sellado de Tiempo</i>	26
7.	Tarifas	27
8.	Auditorías	27
9.	Perfiles de certificados	27
9.1.	<i>Restricciones de los nombres</i>	27
9.2.	<i>Uso de la extensión Policy Constrains</i>	28
9.3.	<i>Sintaxis y semántica de los Policy Qualifiers</i>	28
9.4.	<i>Tratamiento semántico de la extensión "Certificate Policy"</i>	28
Anexo I:	Identificación del certificado de la Autoridades de Certificación	29

Índice de Tablas

Tabla 1 - Identificación de Política de Certificación	7
---	---

1. INTRODUCCIÓN

1. Las presentes *Políticas y Prácticas de Certificación Particulares* describen la emisión o expedición de los *Certificados de Componentes* por parte de la FNMT-RCM. Dichos *Certificados* vinculan unos *Datos de Verificación de Firma* a un *Suscriptor* que tiene el control del funcionamiento del *Componente* que utiliza el *Certificado*.
2. Los *Certificados de Componentes* son aquellos *Certificados* expedidos por la FNMT-RCM bajo la presente *Política de Certificación* y que vinculan unos *Datos de Verificación de Firma* a un *Componente* o aplicación informática sobre la que existe un *Suscriptor*, que actúa como responsable y que tiene el control sobre dicho *Componente* o aplicación. La *Clave Privada* asociada a la *Clave Pública* estará, hasta la instalación del *Certificado de Componente*, bajo la responsabilidad del *Solicitante* y, una vez instalado, bajo la responsabilidad del *Suscriptor*.
3. FNMT-RCM no será responsable de las actuaciones realizadas con este tipo de *Certificados* cuando se produzca abuso de facultades o insuficiencia de las mismas y/o cuando se produzcan decisiones del *Suscriptor* del *Certificado* que afecten a la vigencia de las facultades de su *Representante*, por lo que cualquier modificación, revocación o restricción no será oponible a la FNMT-RCM salvo que sea fehacientemente notificada.
4. Los *Certificados de Componentes* son expedidos y firmados por la FNMT-RCM para ser instalados y utilizados por *Componentes* informáticos, con el objeto de que se herede la confianza que representa la FNMT-RCM como *Prestador de Servicios de Confianza*. Solo podrán obtener *Certificados de Componentes* aquellos *Suscriptores* que hayan suscrito un contrato o convenio con la FNMT-RCM, en virtud del cual formen parte de la *Comunidad Electrónica* tal y como se contempla en la *Declaración de Prácticas de Certificación* de la FNMT-RCM.
5. FNMT-RCM solamente expedirá estos *Certificados* para su uso en el ámbito de la *Comunidad Electrónica* para actuaciones que no resulten incompatibles con el ámbito y uso del *Certificado* correspondiente, al que se encuentre indubitadamente vinculado el *Componente*.
6. La FNMT-RCM, como *Prestador de Servicios de Confianza* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *Suscriptor* que se sirve de tal *Certificado*, no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros respecto de las aplicaciones, sitios web o equipos que se desean proteger con tales *Certificados*, o su uso se presta a engaño o confusión sobre la titularidad de tales *Componentes*. En especial, tal reserva de derechos se podrá ejecutar por la FNMT-RCM cuando en la utilización de tales *Certificados* se atente contra los siguientes principios:
 - La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
 - La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

- El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y
 - La protección de la juventud y de la infancia.
7. La FNMT-RCM quedará exonerada y se mantendrá indemne de cualquier reclamación o reivindicación por el uso inadecuado de los *Certificados de Componentes* que incumpla lo previsto en la *Declaración de Prácticas de Certificación*.

2. ORGANIZACIÓN DEL DOCUMENTO

8. La FNMT-RCM estructura su *Declaración de Prácticas de Certificación* en varios documentos:
- La denominada “*Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM*” (DGPC), que tiene por objeto la información pública de las condiciones y características generales de los servicios de certificación por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*.
 - Cuantos anexos se consideren oportunos para la información pública de las condiciones de uso, limitaciones, responsabilidades, propiedades y cualquier otra información que se considere específica de cada tipo de *Certificado*. Estos anexos tendrán la condición de *Política y Prácticas de Certificación Particulares* del tipo de *Certificado* en cuestión, lo que se refleja en el presente documento para el caso de los *Certificados de Componente*.
9. Por tanto, se considera como *Declaración de Prácticas de Certificación* de un determinado tipo de *Certificado* expedido por la FNMT-RCM al conjunto de los documentos formados por la DGPC y cuantos anexos especifiquen, desarrollen o particularicen las cuestiones relativas al tipo de *Certificado* en cuestión, es decir, la *Política y Prácticas de Certificación* particulares de dicho tipo de *Certificado*
10. Deberá tenerse presente, a efectos interpretativos del presente anexo, el apartado “Definiciones” de la DGPC y el de este documento.
11. El objetivo del presente documento es la información pública del conjunto de prácticas, condiciones y características de los servicios de certificación que presta la FNMT-RCM como *Prestador de Servicios de Confianza*, en relación al ciclo de vida *Certificados* electrónicos de *Componente*.
12. Así pues, el presente documento trae causa y forma parte integrante de la *Declaración de Prácticas de Certificación* de la FNMT-RCM en lo relativo a los *Certificados de Componente*. Contiene la *Política de Certificación* para este tipo de *Certificados*, así como las *Prácticas de Certificación* empleadas en el ciclo de vida de estos.
13. En resumen, estas *Políticas de Certificación y Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la DGPC y, por tanto, son parte integrante de ella, conformando, ambos documentos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM para los *Certificados de Componente*. Así pues, lo descrito en este documento, sólo es de aplicación para el conjunto de *Certificados* caracterizado e

identificado en esta *Política y Prácticas Particulares de Certificación* y pueden revestir, además, especialidades plasmadas a través de la *Ley de Emisión del Certificado* o grupo de *Certificados* correspondiente, en caso de que existan características o funcionalidades específicas.

14. La FNMT-RCM gestiona sus servicios de certificación y emite certificados de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la siguiente dirección <https://cabforum.org/baseline-requirements-documents/>
15. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la correspondiente Declaración de la Política de Certificados para mantenerla acorde a la última versión de los referidos requisitos, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.

3. DEFINICIONES

16. A las definiciones dispuestas en la DGPC, para la interpretación del presente documento se añaden las siguientes:
 - *Certificado de Componente*: Certificado empleado por un *Componente* informático en una infraestructura de clave pública.
 - *Certificado de autenticación de sitio web*: Es un *Certificado de Componente* que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el *Certificado*.
 - *Certificate Transparency (CT)*: es un marco abierto para la supervisión de *Certificados de autenticación de sitio web*, de forma que cuando se expide uno de estos *Certificados*, se publica en registros CT, posibilitando así que los propietarios de dominios puedan supervisar la emisión de los mismos para sus dominios y detectar *Certificados* emitidos erróneamente.
 - *Componente*: Conjunto de elementos informáticos interrelacionados entre sí para transmitir o tratar información y con capacidad de firmarla o cifrarla de manera autónoma.
 - *Registro AAC (CAA records)*: Registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (AAC). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (AC) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de AAC permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada de un *Certificado de autenticación de sitio web* para su nombre de dominio.
 - *Representante*: Administrador, cargo público o apoderado general del *Suscriptor* cuando este es una persona jurídica, órgano u organismo público y que actúa en nombre del *Suscriptor*. Es también la persona física a la que se reconoce la capacidad de autorizar al *Solicitante*.

- *Solicitante*: Persona física que realiza la solicitud relativa al *Certificado* y, en el caso de expediciones, entrega la clave pública a la FNMT-RCM y recibe de esta el certificado.
- *Sujeto del Certificado*: Campo “Subject” del *Certificado* que identifica al *Suscriptor* y al *Componente*.
- *Suscriptor*: Persona jurídica, órgano u organismo público destinatario de las actividades de la FNMT-RCM como *Prestador de Servicios de Confianza*, que suscribe los términos y condiciones del servicio y se referencia en el *Sujeto* en el *Certificado*. Es el titular y responsable del uso del *Certificado* que posee el control exclusivo y la capacidad de decisión sobre el *Componente*.

(Los términos señalados en cursiva se definen en el presente documento o en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica)

4. ORDEN DE PRELACIÓN

17. El orden de prelación es el siguiente:

- Las presentes *Políticas de Certificación y Prácticas de Certificación Particulares de Certificados de Componente* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación, en lo que corresponda y con carácter particular sobre este tipo de *Certificado*, sobre lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

Por tanto, en caso de que existiera contradicción entre el presente documento y lo dispuesto en la DGPC, tendrá preferencia lo aquí articulado.

- La *Ley de Emisión* de cada *Certificado* o grupo de *Certificados* constituirá, en su caso y por su singularidad, norma especial sobre lo dispuesto en las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*. La *Ley de Emisión*, en caso de que se constituya, quedará recogida en el documento de relación a formalizar entre la FNMT-RCM y la *Entidad Usuaria*, y/o en las condiciones de utilización o contrato de expedición y/o en el propio *Certificado*.

5. POLÍTICA DE CERTIFICACIÓN DE LOS CERTIFICADOS DE COMPONENTE

5.1. IDENTIFICACIÓN

18. La presente *Política de Certificación* de la FNMT-RCM para la expedición de *Certificados de Componentes* se descompone en las identificadas a continuación:

Tabla 1 - Identificación de Política de Certificación

Denominación general	<i>Política de Certificación de Certificados de componente</i> de la FNMT-RCM (AC Componentes Informáticos)
----------------------	---



Referencia/OID y nombre específico	1.3.6.1.4.1.5734.3.9.19 – <i>Certificado de componente</i> de sello de entidad 1.3.6.1.4.1.5734.3.9.4 – <i>Certificados de componente</i> de firma de código 1.3.6.1.4.1.5734.3.9.16 – <i>Certificado de autenticación de sitio web</i> estándar 1.3.6.1.4.1.5734.3.9.17 – <i>Certificado de autenticación de sitio web</i> wildcard 1.3.6.1.4.1.5734.3.9.18 – <i>Certificado de autenticación de sitio web</i> multidominio (SAN/UCC) 1.3.6.1.4.1.5734.3.9.14 – <i>Certificados de componente</i> para su uso en las <i>Unidades de Sellado de Tiempo</i> 1.3.6.1.4.1.5734.3.9.20 – <i>Certificado de componente como Unidad de Sellado de Tiempo del Servicio cualificado de Sellado de Tiempo de la FNMT – RCM</i>
Versión	1.7
DPC relacionada	Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM
Localización	http://www.ceres.fnmt.es/dpcs

19. La tabla anterior identifica un OID de política para cada perfil de *Certificado*, aunque todas ellas se describen conjuntamente en este mismo documento. La razón de ello es doble, por un lado, se permite diferenciar de manera automatizada la estructura de campos a interpretar en cada tipo de *Certificado*, y por el otro, se unifican las reglas de aplicación de los *Certificados* a una misma comunidad y con los mismos requisitos de seguridad. Cada una de las políticas se ha relacionado con el tipo de *Certificado*.
20. Los tipos de Certificado contemplados en esta DPC son:
- *Certificado de autenticación de sitio web* estándar: Permite establecer comunicaciones seguras utilizando el protocolo SSL/TSL. Este tipo de *Certificado* garantiza la identidad del dominio de un sitio web.
 - *Certificado de autenticación de sitio web* wildcard: Garantiza la seguridad de un conjunto de subdominios ilimitado, a partir del tercer nivel, con un único *Certificado de autenticación de sitio web*.
 - *Certificado de autenticación de sitio web* multidominio (SAN/UCC): Garantiza la seguridad de un conjunto de dominios independientes entre sí.
 - *Certificado de componente* de firma de código: Permite firmar software y garantizar la identidad del propietario y la integridad del código.
 - *Certificado de componente* de sello de entidad: Se utiliza para la automatización de procesos de firma y autenticación entre componentes informáticos. Además, se permite

al usuario elegir el uso extendido de claves del *Certificado* (autenticación de cliente, protección de correo electrónico).

- *Certificado de componente* para su uso en las *Unidades de Sellado de Tiempo*: Es utilizado por *Autoridades de Sellado de Tiempo* de terceros.
- *Certificado de componente* para su uso en la *Unidad de Sellado de Tiempo* de la FNMT-RCM: Es utilizado por *Autoridades de Sellado de Tiempo* de la FNMT-RCM para prestar el Servicio cualificado de Sellado de Tiempo de dicha Entidad, como Prestador cualificado de Servicios de Confianza. En todo lo relativo a dicho servicio, puede consultarse la Política y Declaración de Prácticas del Servicio de Sellado de Tiempo en la siguiente dirección: <http://www.cert.fnmt.es/dpcs/>

21. El *Certificado de componente* de sello de entidad y el *Certificado de componente* como *Unidad de Sellado de Tiempo* del *Servicio cualificado de Sellado de Tiempo* de la FNMT – RCM, son *Certificados cualificados* de conformidad con el Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

5.2. SEUDÓNIMOS

22. En cuanto a la identificación de los *Suscriptores* mediante el uso de los *Certificados* expedidos bajo la presente *Política de Certificación*, la FNMT – RCM no admite el uso de seudónimos.

5.3. RECONOCIMIENTO Y AUTENTICACIÓN DE MARCAS REGISTRADAS

23. La FNMT – RCM no asume compromiso alguno sobre el uso de marcas comerciales en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación*. No se permite el uso de signos distintivos cuyo derecho de uso no sea propiedad del *Titular* o esté debidamente autorizado, por lo que la FNMT–RCM no está obligada a verificar previamente la titularidad o registro de marcas registradas y demás signos distintivos antes de la emisión de los *Certificados*, aunque figuren en registros públicos.

5.4. COMUNIDAD Y ÁMBITO DE APLICACIÓN

24. La presente *Política de Certificación* es de aplicación en la expedición de *Certificados* electrónicos que tienen las siguientes características:
- Son expedidos por la FNMT-RCM que vinculan unos *Datos de Verificación de Firma* a un *Componente* y a un *Suscriptor* que lo mantiene bajo su control.
 - Los *Certificados* emitidos bajo esta *Política de Certificación* son expedidos para *Entidades usuarias* que forman parte de la *Comunidad Electrónica* tal y como se define en el apartado “Definiciones” de la DGPC de la FNMT-RCM.
 - Los *Certificados* emitidos bajo esta *Política de Certificación* se consideran idóneos como parte integrante de sistemas de firma electrónica que requieran niveles de seguridad específicos y, en especial, para el establecimiento de comunicaciones

seguras entre una dirección electrónica y el usuario que se conecte a ella, además de ser una herramienta para autenticar e identificar a la dirección electrónica para la cual han sido emitidos.

5.4.1. Participantes

25. A efectos de las presentes *Políticas y Prácticas de Certificación Particulares*, la *Autoridad de Certificación* es la FNMT – RCM, como Prestador de Servicios de Confianza.
26. La Autoridad de Registro a los efectos de la realización de operaciones de registro será la propia FNMT-RCM, que ejercerá como única *Oficina de Registro* autorizada, a través de su Área de Registro.
27. Las entidades suscriptoras de los certificados, que son las personas jurídicas, órganos u organismos públicos que tienen bajo su control y operación el dominio identificado por el *Certificado de autenticación de sitio web* o, en el caso de los *Certificados de componente* de sello de entidad, son los creadores del mismo. Por tanto, estas entidades son titulares y responsables del uso del *Certificado*, con control exclusivo y capacidad de decisión sobre el *Componente*.
28. Terceras partes que confían en los *Certificados* emitidos bajo esta *Política de Certificación*: son las personas que voluntariamente confían en dichos *Certificados* en virtud de la confianza depositada en la FNMT – RCM, como Prestador de Servicios de Confianza.

5.5. RESPONSABILIDADES Y OBLIGACIONES DE LAS PARTES

29. Esta *Política de Certificación* recoge las obligaciones y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados de Componente*, expedidos bajo la presente *Política*.
30. FNMT-RCM no será responsable de la utilización de los *Certificados de Componente* cuando el *Suscriptor* del *Certificado* y, en su caso, su *Representante*, realice actuaciones sin facultades, extralimitándose en las mismas o en fraude de ley o de terceros, si no existe notificación fehaciente que permita trasladar los efectos pretendidos a la gestión de los *Certificados*.

5.5.1. Responsabilidades de las partes

31. Para poder usar *Certificados* expedidos por la FNMT-RCM se deberá previamente formar parte de la *Comunidad Electrónica* y adquirir la condición de *Entidad Usuaria*. Para confiar en un *Certificado de Componente*, será imprescindible comprobar el estado de validez del *Certificado* mediante el *Servicio de Información y Consulta sobre el estado de los Certificados* de la FNMT – RCM.
32. De producirse esta confianza por parte de un miembro de la *Comunidad Electrónica*, *Entidad Usuaria* o por parte de un tercero, sin realizar la comprobación del estado del *Certificado*, no se obtendrá cobertura de la *Declaración de Prácticas de Certificación*, y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM. Por tanto, en tal caso, esta Entidad no será responsable de los por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado de Componente*.

5.5.1.1. Responsabilidad del Prestador de Servicios de Confianza

33. La FNMT-RCM únicamente responde de la correcta identificación personal del *Solicitante*, *Suscriptor* y, en su caso, del *Representante*. Respecto de esta información, la FNMT-RCM se limita únicamente a expresarla en un *Certificado* para el que se le ha acreditado la identidad de su *Suscriptor*.
34. La FNMT-RCM responde de realizar la comprobación, en las bases de datos correspondientes, de que el *Suscriptor* es el titular de los nombres de dominio consignados en la solicitud del *Certificado*.
35. La FNMT-RCM únicamente responderá por deficiencias en los procedimientos propios de su actividad como *Prestador de Servicios de Confianza*, y conforme a lo dispuesto en estas *Políticas de Certificación* o en la Ley. En ningún caso será responsable de las acciones o de las pérdidas en las que incurran, *Solicitantes*, *Suscriptores*, *Representantes*, *Entidades usuarias*, o, en su caso, terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los mencionados procedimientos de expedición y/o de gestión de los *Certificados*.
36. FNMT-RCM no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT podrá establecer cláusulas de limitación de responsabilidad adicionales a las recogidas en este documento.
37. La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización de los *Certificados* haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la *Declaración de Prácticas de Certificación*, y en especial lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.
38. La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente.
39. La FNMT-RCM no garantiza los algoritmos criptográficos, ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo con el estado actual de la técnica, y procedió conforme a lo dispuesto en esta *Declaración de Prácticas de Certificación* y en la Ley.
40. Para el caso específico de los *Certificados de Componente* para su uso en las *Unidades de Sellado de Tiempo* pertenecientes a *Autoridades de Sellado de Tiempo* de terceros, se hace constar que la FNMT-RCM no tendrá responsabilidad alguna, ni garantizará, ningún aspecto del servicio de *Sellado de Tiempo* que puedan ofrecer las entidades titulares de tales *Unidades* y *Autoridades de Sellado de Tiempo*. En especial la exención de responsabilidad alcanzará a la gestión de cualquiera de los aspectos relacionados con los sistemas de información empleados por dichas *Unidades* o *Autoridades*, así como la validez de las fuentes de tiempo, o su sincronismo, empleadas en el servicio.
41. En todo caso y con la condición de cláusula penal, la cuantía que la FNMT-RCM debiera satisfacer, en concepto de daños y perjuicios, por imperativo judicial a terceros perjudicados

o miembro de la *Comunidad Electrónica*, en defecto de regulación específica en los contratos o convenios, se limita a un máximo de SEIS MIL EUROS (6.000€).

5.5.1.2. Responsabilidad del Solicitante

42. El *Solicitante* responderá de la veracidad y exactitud de la información presentada durante la solicitud del *Certificado*, de que cuenta con autorización o apoderamiento del *Suscriptor* para realizar la solicitud y de que instalará adecuadamente el *Certificado* en el *Componente* designado por el *Suscriptor*.
43. El *Solicitante* mantendrá a salvo y defenderá a su costa a la FNMT-RCM contra cualquier acción que pudiera emprenderse contra esta Entidad y contra cualquier daño y perjuicio que sufra la FNMT – RCM como consecuencia de la inadecuada instalación del *Certificado*, falsedad o errores graves sobre la información suministrada en el procedimiento de expedición del *Certificado*, o como consecuencia de un acto u omisión culposa o negligente del *Solicitante*.

5.5.1.3. Responsabilidad del Suscriptor

44. Será en todo caso responsabilidad del *Suscriptor* utilizar de manera adecuada y custodiar diligentemente el *Certificado*, según el propósito y función para el que ha sido expedido, así como informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.
45. Asimismo, será el *Suscriptor* quien deba responder, en todo caso, ante la FNMT-RCM, las *Entidades usuarias* y, en su caso, ante terceros, del uso indebido del *Certificado*, o de la falsedad o errores de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.
46. Será responsabilidad y, por tanto, obligación del *Suscriptor* no usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* que realizó la expedición del *Certificado* en cuestión y no se hubiera producido la subrogación prevista en la ley. En todo caso, el *Suscriptor* no usará el *Certificado* en los casos en los que los *Datos de Creación de Firma* del *Prestador* puedan estar amenazados y/o comprometidos, y así se haya comunicado por el *Prestador* o, en su caso, hubiera tenido noticia de estas circunstancias.
47. En el caso de *Certificados* para *Unidades de Sellado de Tiempo* expedidos por la FNMT-RCM a terceros (Entidades que se erigirán como *Autoridad de Sellado de Tiempo* para prestar un *Servicio de Sellado de Tiempo*), será responsabilidad de dichas Entidades garantizar, en su caso, la validez del mismo de conformidad con las normas técnicas y la legislación vigente, quedando exenta la FNMT-RCM de toda responsabilidad relativa a la prestación del citado *Servicio de Sellado de Tiempo*. FNMT-RCM se limita, en este caso, a la expedición de un *Certificado electrónico*, con capacidad técnica para expedir *Sellos de tiempo electrónicos*, a nombre de la Entidad debidamente acreditada.
48. Un caso concreto de *Certificado* para *Unidades de Sellado de Tiempo* es el que utiliza la FNMT-RCM para proveer su *Servicio de Sellado de Tiempo*, como *Prestador cualificado de servicios de confianza*, según la *Política y Prácticas del Servicio Cualificado de Sellado de*

*Tiempo*¹, y de conformidad con el estándar europeo ETSI EN 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

5.5.1.4. Responsabilidad de la Entidad Usuaria y terceros que confían

49. Será responsabilidad de la *Entidad usuaria*, de los terceros que confían en los *Certificados* y, en general de los miembros de la *Comunidad Electrónica*, la verificación y comprobación del estado de los *Certificados*, no cabiendo en ningún caso presumir la validez de los *Certificados* sin dichas comprobaciones.
50. No podrá considerarse que la *Entidad usuaria* y terceros que confían en los *Certificados* han actuado con la mínima diligencia debida si confían en una *Firma Electrónica* basada en un *Certificado* expedido por la FNMT-RCM sin haber observado lo dispuesto en la *Declaración de Prácticas de Certificación* y comprobado que dicha *Firma Electrónica* puede ser verificada por referencia a una *Cadena de Certificación* válida.
51. Si las circunstancias indican necesidad de garantías adicionales, la *Entidad Usuaria* deberá obtener garantías adicionales para que dicha confianza resulte razonable.
52. Asimismo, será responsabilidad de la *Entidad Usuaria* observar lo dispuesto en la *Declaración de Prácticas de Certificación* y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados* en esta *Política de Certificación*.

5.5.2. Obligaciones y garantías de las partes

5.5.2.1. Obligaciones y Garantías del Prestador de Servicios de Confianza

53. La FNMT-RCM no estará sujeta a otras garantías ni otras obligaciones que las establecidas en la normativa sectorial de aplicación y en la *Declaración de Prácticas de Certificación*.
54. Sin perjuicio de lo dispuesto en la legislación sobre firma electrónica, y su normativa de desarrollo, así como en su normativa específica, el *Prestador de Servicios de Confianza* se obliga a:
55. Con carácter previo a la expedición del *Certificado*:
 - Comprobar la identidad y circunstancias personales del *Solicitante* del *Certificado* y del *Suscriptor* y/o su *Representante* y recoger la manifestación de que el *Solicitante* está autorizado por el *Suscriptor* para realizar la solicitud. En ningún caso se expedirán *Certificados* a menores de edad, salvo que ostenten la cualidad de emancipados.

La identificación se realizará a través de certificados de firma electrónica admitidos y de las funcionalidades previstas respecto del DNIE a los efectos antes señalados.

¹ Véase la Declaración de Prácticas del Servicio Cualificado de Sellado de Tiempo en <http://www.cert.fnmt.es/dpcs/>

- En el proceso de registro, comprobar los datos relativos a la personalidad jurídica del *Suscriptor* y a la capacidad del *Representante*. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los protocolos y procedimientos de registro de la FNMT-RCM.

En los procesos de comprobación de los extremos antes señalados anteriormente la FNMT-RCM podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de registros públicos o privados.

- Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.
- Comprobar que el *Solicitante* está en posesión de la *Clave Privada* que constituirá, una vez expedido el *Certificado*, los *Datos de Creación de Firma / Sello* correspondientes a los de *Datos de Verificación de Sello* que constarán en el *Certificado*, y comprobar su complementariedad.
- Garantizar que los procedimientos seguidos aseguran que las *Claves Privadas* que constituyan los *Datos de Creación de Sello* son generados sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de la FNMT-RCM.
- Realizar la comunicación de información al *Suscriptor*, *Representante* y *Solicitante* de tal forma que se procure su *Confidencialidad*.
- Poner a disposición del *Solicitante*, *Suscriptor*, *Representante* y demás interesados (<http://www.ceres.fnmt.es>) la *Declaración de Prácticas de Certificación* y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los *Certificados* objeto de esta *Política de Certificación* y *Prácticas de Certificación Particulares* de conformidad con la normativa aplicable.

56. Conservación de la información por la FNMT-RCM

- Conservar toda la información y documentación relativa a cada *Certificado*, en las debidas condiciones de seguridad, durante quince (15) años contados desde el momento de su expedición.
- Mantener un *Directorio* seguro y actualizado de *Certificados* en el que se identifican los *Certificados* expedidos, así como su vigencia, incluyendo en forma de *Listas de Revocación* la identificación de los *Certificados* que hayan sido revocados. La integridad de este *Directorio* se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España y, en su caso, de la UE.
- Mantener un servicio de información y consulta sobre el estado de los *Certificados*.
- Establecer un mecanismo de fechado que permita determinar con exactitud la fecha y la hora en las que se expidió un *Certificado*, o se extinguió su vigencia.
- Conservar la *Declaración de Prácticas de Certificación* durante 15 años desde su derogación por publicación de una nueva versión de la misma, en las debidas condiciones de seguridad.

57. Protección de los Datos de Carácter Personal:

- La FNMT-RCM se compromete a cumplir la legislación vigente en materia de Protección de Datos de Carácter Personal, fundamentalmente, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Para informarse sobre la política de protección de datos seguida por la FNMT-RCM, y acerca del uso que de los datos se realiza, se puede consultar la DGPC.

58. Revocación de *Certificados*:

- Acerca de la revocación de *Certificados* y de las obligaciones que la FNMT-RCM se compromete a asumir al respecto, se puede consultar el procedimiento de revocación de *Certificados* reflejado en el presente documento.

59. Cese de la actividad de la FNMT-RCM como *Prestador de Servicios de Confianza*:

- A este respecto se puede consultar el apartado correspondiente de la DGPC.

5.5.2.2. *Obligaciones de la Oficina de Registro*

60. Para la gestión del ciclo de vida de los *Certificados de Componente*, la FNMT-RCM será la única *Oficina de Registro* autorizada, a través de su Área de Registro, teniendo como obligaciones:

- Con carácter general, seguir los procedimientos establecidos por la FNMT-RCM en la *Política y Prácticas de Certificación* de aplicación en el desempeño de sus funciones de gestión, expedición y revocación de *Certificados* y no alterar dicho marco de actuación.
- En particular, comprobar la identidad y cualesquiera circunstancias personales de los *Solicitantes, Suscriptores y Representantes* de los *Certificados* relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en Derecho y conforme a lo previsto con carácter general en la DGPC y con carácter particular en la presente *Política y Prácticas de Certificación Particulares*.
- Comprobar que la titularidad del nombre de dominio se corresponde con la identidad del *Suscriptor* o, en su caso, obtener la autorización de éste, que se asociará al *Certificado de Componente*, por los medios a su alcance que, razonablemente, permitan acreditar tal titularidad, de conformidad con el estado de la técnica.
- Recoger expresamente la manifestación del *Suscriptor* en relación con la titularidad del *Componente*, manifestando que tiene el poder único de decisión sobre el mismo.
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación o revocación gestiona durante quince (15) años.

- Realizar la recepción y gestión de las solicitudes y los contratos de expedición (formulario pdf) de *Certificados* con el *Suscriptor* de los mismos.
- Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.

5.5.2.3. *Obligaciones del Solicitante y Suscriptor*

61. El *Solicitante* y el *Suscriptor* de los *Certificados* expedidos bajo la presente *Declaración de Prácticas de Certificación*, tienen la obligación de:

- No usar el *Certificado* fuera de los límites especificados en la presente *Política y Prácticas de Certificación* particulares.
- No usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado su actividad como Entidad emisora de *Certificados* que expidió el certificado en cuestión, especialmente en los casos en los que los *Datos de Creación de Sello* del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- No solicitar para el *Sujeto* del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciataria o cuenta con autorización demostrable para su uso.
- Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma / Sello* o cualquier otra información sensible como *Claves*, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados*, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM, las circunstancias para la revocación o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de los *Datos de Creación de Firma*,
- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados*, el *Sello electrónico avanzado* del *Prestador de Servicios de Confianza* emisor del *Certificado*.

- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.
- Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.

5.5.2.4. Obligaciones de la Entidad Usuaria y terceros que confían

62. Las *Entidades Usuaras*, los miembros de la *Comunidad Electrónica* y, en general, los terceros que confían en los *Certificados* expedidos bajo la presente *Declaración de Prácticas de Certificación*, tienen la obligación de:
- Verificar con carácter previo a confiar en los *Certificados*, el *Sello Electrónico* avanzado del *Prestador de Servicios de Confianza* emisor del *Certificado*.
 - Verificar que el *Certificado* del *Suscriptor* continúa vigente y activo.
 - Verificar el estado de los *Certificados* en la *Cadena de Certificación*, a través del *Servicio de Información y Consulta sobre el Estado de los Certificados* de la FNMT-RCM.
 - Comprobar las limitaciones de uso del *Certificado* que se verifica.
 - Conocer las condiciones de utilización del *Certificado* conforme a las *Políticas y Declaraciones de Prácticas de Certificación* de aplicación.
 - Notificar a la FNMT-RCM cualquier anomalía o información relativa al *Certificado* y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

5.6. LÍMITES DE USO DE LOS CERTIFICADOS Y ACEPTACIÓN DEL MISMO

63. FNMT-RCM no será responsable de *Certificados* con apariencia fraudulenta de haber sido expedidos por la FNMT-RCM y emprenderá las acciones legales contra estas actuaciones fraudulentas si tuviera conocimiento de las mismas, directamente o por denuncia de los interesados.
64. Si un miembro de la *Comunidad Electrónica*, una *Entidad Usuaria* o un tercero confiaran en un *Certificado de Componente* sin realizar la comprobación del estado del *Certificado*, no se obtendrá cobertura de la presente *Declaración de Prácticas de Certificación* y se carecerá de legitimidad alguna para reclamar o emprender acciones judiciales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado de Componente*.
65. Además, incluso dentro del ámbito de la *Comunidad Electrónica*, no se podrán emplear este tipo de *Certificados*, por persona distinta a la FNMT-RCM, para:
- Firmar otro *Certificado*.

- Generar *Sellos de Tiempo* para procedimientos de *Sellado de Tiempo* –a excepción de los *Certificados* expedidos por la FNMT-RCM para *Unidades de Sellado de Tiempo*–.
- Prestar servicios a título gratuito u oneroso, como por ejemplo serían a título enunciativo:
 - Prestar servicios de *OCSP*.
 - Prestar servicios de facturación electrónica.
 - Generar *Listas de Revocación*.
 - Prestar servicios de notificación.

6. PRÁCTICAS DE CERTIFICACIÓN PARTICULARES PARA LOS CERTIFICADOS DE COMPONENTE “AC COMPONENTES INFORMÁTICOS”

66. Estas *Prácticas de Certificación Particulares* para los *Certificados de Componente* definen el conjunto de prácticas adoptadas por la FNMT-RCM como *Prestador de Servicios de Confianza* para la gestión del ciclo de vida de los *Certificados* expedidos bajo la *Política de Certificación de Certificados* de componente de la FNMT-RCM.

6.1. GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS DE COMPONENTE

67. Se definen aquí aquellos aspectos que, si bien ya han sido apuntados en la DGPC de la que este documento forma parte, revisten determinadas especialidades que necesitan un mayor nivel de detalle.

6.1.1. Procedimiento de solicitud

68. En el procedimiento de solicitud se toman los datos personales del *Solicitante de Certificado de Componente*, del *Suscriptor* y, en su caso, su *Representante*. Además, se verifica la información específica que ha de contener el *Certificado* y se formaliza su contrato con la FNMT-RCM para su posterior expedición. Como desarrollo de este esquema existirá un procedimiento de registro detallado, poniéndose a disposición de los *Solicitantes* los aspectos necesarios para la solicitud del *Certificado*. Estas actividades serán realizadas únicamente por la *Oficina de Registro* autorizada.
69. La FNMT-RCM comprueba si hay un *Registro AAC* para cada nombre de dominio que incluye en un *Certificado de autenticación de sitio web* emitido, de acuerdo con el procedimiento establecido en RFC 6844 y siguiendo las instrucciones de procesamiento establecidas en RFC 6844 para cualquier registro encontrado. Si existe dicho *Registro AAC*, no emitirá dicho *Certificado* a menos que determine que la solicitud del *Certificado* es consistente con el conjunto de registro de recursos AAC aplicable.
70. El *Suscriptor* (a través del *Solicitante*) genera las *Claves pública y privada* y realiza la solicitud del *Certificado* a través de un formulario web de la FNMT-RCM, que deberá incluir:
- Los datos identificativos del *Componente*

- Los datos relativos a la titularidad de los Nombres de Dominio, o manifestación de titularidad del *Componente*, que se vincularán a cada tipo de *Certificado*
- Los datos correspondientes al *Suscriptor* como persona o entidad interesada en la expedición de un *Certificado de Componente*, ya sea pública o privada.
- Los datos correspondientes al *Representante* del *Suscriptor* del *Certificado* cuando el *Suscriptor* sea una entidad.
- Los datos del *Solicitante* del *Certificado*
- El PKCS#10 o SPKAC de la petición del *Certificado de Componente*

71. En cualquier caso, se completarán todos los campos del formulario que sean consignados como obligatorios y el formulario en su totalidad será firmado electrónicamente por el *Solicitante*, firma que será verificada por la FNMT-RCM.

6.1.2. Suscripción y envío del contrato por el *Suscriptor*

72. Tras la solicitud, el *Suscriptor* firmará electrónicamente el contrato (formulario pdf, donde consta la aceptación de las condiciones de uso del *Certificado* solicitado y que estará disponible en la página web correspondiente) y lo remitirá, a través de la dirección electrónica proporcionada, a la *Oficina de Registro* de la FNMT-RCM para su tratamiento.

73. La firma del contrato pdf se realizará, preferentemente, con el *Certificado de representante de Persona Jurídica* del *Suscriptor* expedido por la FNMT-RCM, pudiéndose utilizar otros *Certificados* admitidos.

74. No remitir el contrato firmado por el *Suscriptor*, no realizar el pago, la ausencia de datos o de la documentación exigida, serán causas de interrupción del proceso de expedición del *Certificado*.

75. La FNMT-RCM conservará la copia firmada por el *Suscriptor* y la archivará junto con toda la documentación referida a ese *Componente* informático.

76. La *Oficina de Registro* de la FNMT-RCM, durante el proceso de registro, verifica toda la información relativa a la identidad del titular del *Certificado*.

6.1.3. Validación del dominio

77. Para validar el dominio de los *Certificados de autenticación de sitio web*, la FNMT-RCM utiliza alguno de los siguientes métodos descritos en el documento CA/Browser Forum's Baseline Requirements: "3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact", "3.2.2.4.3 Phone Contact with Domain Contact", "3.2.2.4.4 Constructed Email to Domain Contact" o "3.2.2.4.6 Agreed-Upon Change to Website.

78. La FNMT-RCM confirma que el *Solicitante* posee el control sobre los nombres completos de los dominios o FQDN (siglas en inglés de Fully Qualified Domain Name) que son incorporados a los *Certificados de autenticación de sitio web* que expide. Para ello, la FNMT-RCM consulta, a través de la aplicación que registra las solicitudes de estos *Certificados*, la identidad del *Solicitante* y el nombre del citado FQDN. A continuación, verifica que la solicitud proviene del contacto que tiene el control sobre dicho dominio

(según los métodos definidos en el apartado anterior) o tiene autorización por parte de este. Adicionalmente se comprueba que la solicitud del *Certificado* ha sido realizada con posterioridad al alta en dichos registros.

79. Adicionalmente, antes de la emisión de un *Certificado de autenticación de sitios web*, se verifica que el dominio a incluir en el *Certificado* es público (no es un dominio interno) y se consulta a registros públicos para verificar que no es un dominio de alto riesgo (por ejemplo, el registro de Google creado para este fin, como es Safe Browsing site status).
80. Para aquellos *Certificados* que incorporen más de un nombre de dominio (*Certificados multidominio*), se realizarán las comprobaciones correspondientes para todos y cada uno de los nombres de dominio incorporados al *Certificado*. Si alguno de dichos nombres de dominio no cumpliera con los requisitos que se verifican con las comprobaciones realizadas, no se expedirá el *Certificado*.

6.1.4. Expedición

81. Los procesos relativos a la emisión de *Certificados* electrónicos garantizan que todas las cuentas que intervienen en los mismos tienen autenticación multi-factor.
82. La FNMT-RCM mantiene una base de datos interna de todos los *Certificados* revocados y de todas las solicitudes de *Certificados* rechazadas previamente debido a sospecha de phishing u otro uso fraudulento. Esta información es tenida en cuenta para identificar posteriores solicitudes de *Certificados* sospechosos antes de proceder a la aprobación de la expedición de los mismos.
83. Adicionalmente, FNMT-RCM desarrolla, mantiene e implementa procedimientos documentados que identifican y requieren actividad de verificación adicional para las solicitudes de *Certificados* de alto riesgo antes de la aprobación de la expedición del *Certificado*, según sea razonablemente necesario para garantizar que dichas solicitudes se verifican adecuadamente según estos requisitos.
84. La FNMT-RCM comprobará la veracidad de los datos incluidos en la solicitud y, en su caso, la capacidad del *Representante* a través de las verificaciones correspondientes y conservando las evidencias oportunas.
85. La firma electrónica generada para la suscripción del contrato será verificada por la FNMT-RCM.
86. La FNMT-RCM, una vez recibida en su Oficina de Registro la solicitud web y el contrato, dará curso a la petición mediante sus aplicaciones informáticas internas.
87. Si el *Certificado* estuviera asociado a uno o varios dominios de Internet, la *Oficina de Registro* comprobará la existencia y singularidad de dichos dominios mediante consulta a la Internet Corporation for Assigned Names and Numbers (ICANN) y que el *Representante* posee el derecho de uso de dichos dominios o subdominios mediante consulta a las bases de datos de los registradores autorizados de dominios (whois.icann.org, www.nic.es, www.eurid.eu...), conservando evidencias de dicha consulta.
88. La *Oficina de Registro* verificará la personalidad del *Suscriptor* y, en su caso, la personalidad y capacidad del *Representante* mediante la verificación de las *Firmas*

Electrónicas y Certificados utilizados en el proceso y/o consulta de las bases de datos del Registro Mercantil o de terceras partes de confianza.

89. En caso de que existan errores o contradicciones, la FNMT-RCM contactará con el *Solicitante* y *Suscriptor* para su aclaración y, en su caso, subsanación.
90. La FNMT-RCM, por medio de su *Sello Electrónico*, suscribirá la información contenida en los *Certificados* que expida dotándola así de autenticidad e integridad.
91. La FNMT-RCM actuará para:
 - Comprobar que el *Solicitante* del *Certificado* posee la *Clave Privada* correspondiente a la *Clave Pública* a certificar, y que el tamaño de las claves generadas es correcto.
 - Determinar que la información incluida en el *Certificado* se base en la información proporcionada por el *Solicitante* y el *Suscriptor* y que, utilizando una normal diligencia en la realización de las comprobaciones, tal información es veraz.

6.1.5. Publicación y distribución

92. La entrega del *Certificado* se realiza, previa notificación, poniéndolo a disposición del *Solicitante* en la aplicación de descarga de *Certificados* una vez sean cumplidos el resto de requisitos para su expedición.
93. La FNMT – RCM pondrá a disposición del *Solicitante* el *Certificado* en un periodo de tiempo máximo de 72 horas desde la recepción en la *Oficina de Registro* de la documentación necesaria para realizar las verificaciones previas a la expedición.
94. Los *Certificados de autenticación de sitio web* emitidos bajo las presentes políticas se publican en los registros del servicio *Certificate Transparency* de aquellos proveedores con los que la FNMT-RCM mantiene un acuerdo para tal fin.

6.1.6. Notificación al solicitante

95. La FNMT – RCM comunica al *Solicitante* del *Certificado* la puesta a su disposición del mismo mediante el envío de un correo electrónico dirigido al *Representante* del *Suscriptor* del *Certificado* y al *Solicitante*.
96. La FNMT-RCM no realiza ninguna notificación sobre la emisión de *Certificados* a otras entidades.

6.1.7. Vigencia

6.1.7.1. Caducidad

97. El periodo de vigencia máxima de los *Certificados de autenticación de sitio web* (estándar, multidominio y wildcard), es de dos años contados a partir del momento de su expedición. Para los *Certificados de Componente* de sello de entidad y de firma de código dicho periodo es de tres años. En el caso de los *Certificados para Unidades de Sellado de Tiempo* el periodo de vigencia máxima es de cinco años. Dichos periodos de vigencia máxima se

mantienen, siempre y cuando no se vean afectados por las causas y procedimientos expuestos en el apartado “Extinción de la vigencia del Certificado”.

6.1.7.2. Extinción de la vigencia del Certificado

98. Los *Certificados de Componente* expedidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

- a) Terminación del período de validez del *Certificado*.
- b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

En estos dos casos [a) y b)], la pérdida de eficacia de los *Certificados* tendrá lugar desde que estas circunstancias se produzcan.

- c) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

99. A los efectos enumerados anteriormente, se hace constar que la solicitud de expedición de un *Certificado de Componente*, cuando exista otro vigente con los mismos datos de identificación y perteneciente a la misma *Ley de Emisión*, no producirá la revocación del primero obtenido. Por tanto, podrán existir varios *Certificados* en vigor con el mismo *Sujeto*, pero diferente número de serie.

100. Los efectos de la extinción de vigencia del *Certificado* por revocación, surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo haga constar en la *Lista de Revocación* de su *Servicio de Información y Consulta sobre el estado de validez de los Certificados*.

6.1.8. Renovación

101. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no renueva *Certificados*.

6.1.9. Revocación

102. La solicitud de revocación de los *Certificados de Componente* podrá efectuarse durante el período de validez que consta en el *Certificado*. Consiste en la cancelación de la garantía de identidad u otras propiedades del usuario y su correspondencia con la *Clave Pública* asociada.

103. La revocación de un *Certificado de Componente*, sin perjuicio de las causas de revocación que se señalan a continuación, sólo podrá ser solicitada por el *Suscriptor*.

104. La FNMT-RCM pone a disposición de los *Suscriptores*, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM

<https://www.sede.fnmt.gob.es/>

con instrucciones claras, para permitirles reportar cualquier asunto relacionado con este tipo de *Certificados*, en cuanto a un supuesto compromiso de *Clave Privada*, uso indebido de los *Certificados* u otros tipos de fraude, compromiso, mal uso o conducta inapropiada.

6.1.9.1. Causas de revocación

105. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:
- Que la revocación le haya sido solicitada por el *Suscriptor* siguiendo el procedimiento establecido a tal efecto.
 - Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
 - Que, en las causas c) a e) del siguiente apartado, le sean acreditados dichos extremos fehacientemente, previa identificación del solicitante de la revocación (el *Suscriptor*).
106. Teniendo en cuenta lo anterior, serán causas de revocación de un *Certificado de Componente*:
- a) La solicitud de revocación por parte del *Suscriptor* o un tercero debidamente autorizado, realizada de manera fehaciente. En todo caso deberá dar lugar a esta solicitud:
 - Pérdida del soporte del *Certificado*.
 - La utilización por un tercero de los *Datos de Creación de Firma*, asociados a los *Datos de Verificación de Firma* contenidos en el *Certificado* y vinculados a la identidad del *Suscriptor*.
 - La puesta en peligro de los *Datos de Creación de Firma*.
 - La no aceptación de las nuevas condiciones tras la redacción y publicación de nuevas versiones de *Declaraciones de Prácticas de Certificación* o de *Políticas y Prácticas Particulares*, durante el periodo de un mes tras su publicación.
 - b) Resolución judicial o administrativa que así lo ordene.
 - c) Fallecimiento, extinción o disolución de la personalidad jurídica del *Suscriptor*.
 - d) Incapacidad sobrevenida, total o parcial, del *Suscriptor*.
 - e) Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado*, o alteración de los mismos, especialmente si el nombre del dominio consignado en el *Certificado* ya no está bajo el control del *Suscriptor*.
 - f) Solicitar para el Sujeto del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que el *Suscriptor* no sea titular, licenciatario o usuario autorizado.
 - g) El impago de los servicios prestados.

- h) Contravención de una obligación sustancial de esta *Política de Certificación* por parte del *Suscriptor del Certificado* que haya sido conocida por la FNMT-RCM o por parte de la *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.
 - i) Puesta en peligro del secreto de los *Datos de creación de Firma* de la FNMT-RCM, con los que firma los *Certificados* que emite.
 - j) Utilizar el *Certificado* con el propósito de generar dudas a los usuarios sobre la procedencia de los productos o servicios ofertados, haciendo ver que su origen es distinto del realmente ofertado. Para ello, se seguirán los criterios sobre actividad infractora de las normas sobre consumidores y usuarios, comercio, competencia y publicidad.
 - k) Incumplimiento de los requisitos definidos por los esquemas de auditorías a los que se somete la Autoridad de Certificación “AC Componentes Informáticos”, con especial atención a los de algoritmia y tamaños de clave, que supongan un riesgo inaceptable por parte de las partes que confían en estos *Certificados*.
107. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a f) del presente apartado. Para el resto de supuestos, se entenderá que son efectivos desde que son conocidos por la FNMT-RCM.
108. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado*, las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.
109. La falta de adecuación de los datos a la realidad, cuando estos datos se encuentren en Registros públicos no serán imputables a la FNMT-RCM hasta tanto no existan instrumentos de comunicación telemática directa de la FNMT-RCM con los diferentes Registros públicos, salvo que se proceda a su comunicación a la FNMT a través de medios fehacientes.

6.1.9.2. Procedimiento para la revocación de Certificados

110. Existe un servicio de atención telefónica, en horario 24 x 7, en el teléfono 902 200 616, al que se pueden dirigir las solicitudes de revocación. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.
111. Para solicitar una revocación telefónica de un *Certificado*, el *Solicitante* de la misma debe ser el *Suscriptor* o su representante en el caso de personas jurídicas u organismos públicos, y debe aparecer como tal en el certificado a revocar. En el caso del representante, este debe ser la misma persona que actuó como tal en la solicitud de expedición del certificado objeto de la revocación.
112. Adicionalmente, el *Solicitante* de la revocación podrá dirigir su solicitud a la *Oficina de Registro* de la FNMT-RCM, siguiendo el siguiente procedimiento:
1. Solicitud del *Suscriptor*

El *Suscriptor* enviará el formulario de solicitud de revocación, cumplimentado y firmado electrónicamente a la FNMT-RCM, con los mismos *Certificados* que son admitidos para la solicitud y por los canales electrónicos habilitados por esta Entidad.

2. Tramitación de la solicitud por la FNMT-RCM

El registrador de la FNMT-RCM recibirá el contrato de revocación y realizará las mismas comprobaciones relativas a la identidad y capacidad del *Suscriptor* y *Representante* que para el caso de la solicitud de expedición y, si procediera, tramitará la revocación del *Certificado de Componente*.

Tan pronto se resuelva la revocación, el *Suscriptor* recibirá a través de la dirección de correo electrónico consignada en la solicitud, la notificación de la revocación del *Certificado*.

Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Revocación*, conteniendo el número de serie del *Certificado* revocado, la fecha y hora de revocación y la causa de revocación.

113. La FNMT – RCM, aunque no haya recibido la solicitud de revocación por parte del *Suscriptor*, procederá a revocar aquellos *Certificados* de los que obtenga evidencias de estar incluidos en alguna de las causas de revocación previstas en la presente *Declaración de Políticas y Prácticas de Certificación Particulares*.

6.1.9.3. Efectos y periodo de la revocación

114. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes, y así lo haga constar en la *Lista de Revocación* y en su *Servicio de Información y Consulta sobre el Estado de los Certificados*.
115. La revocación del *Certificado* se produce de manera inmediata desde la recepción del contrato de revocación o desde la acreditación telefónica del solicitante.

6.1.10. Suspensión

116. No se permite la suspensión de estos tipos de *Certificados*.

6.1.11. Información del cambio de estado del Certificado

117. Una vez se ha hecho efectiva la revocación del *Certificado*, FNMT-RCM envía una comunicación a la dirección de correo electrónico del *Representante* del *Suscriptor* del *Certificado*, informando del cambio de estado del *Certificado*.

6.1.12. Comprobación del estado del Certificado

118. El *Suscriptor* del *Certificado* y los terceros que confían en los *Certificados* podrán realizar la comprobación del estado de un *Certificado* en la forma y condiciones que se expresan en este apartado.

119. El estado del *Certificado de Componente* se podrá comprobar a través del *Servicio de información y consulta del estado de los certificados* mediante el protocolo OCSP.
120. Estos servicios estarán disponibles las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección <http://www.ceres.fnmt.es> si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.
121. La FNMT-RCM dispone de un servicio de respuesta OCSP ("OCSP responder") para ofrecer el *Servicio de información y consulta del estado de los certificados*.
122. El servicio funciona de la siguiente manera: el servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* registrado en el sistema o por una aplicación comercial (por ejemplo, un navegador web) que extrae del propio certificado (campo Authority Info Access) el enlace a este servicio. Dicho servidor OCSP comprueba el estado de los *Certificados* incluidos en la petición y, en el caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición.
123. Será responsabilidad de la Entidad usuaria obtener un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.
124. Es responsabilidad de la entidad usuaria solicitante del servicio OCSP obtener, en su caso, el consentimiento del *Suscriptor* del *Certificado* sobre el que se solicita el servicio OCSP, así como informarle de las condiciones y limitaciones correspondientes.
125. Lo anterior se entiende con el alcance y límites de la legislación sobre tratamiento automatizado de datos de carácter personal y de conformidad con los correspondientes contratos, convenios o *Leyes de Emisión* por los que se regula el servicio de certificación electrónica de la FNMT-RCM.
126. FNMT-RCM no proporciona servicio de comprobación de *Certificados* de otros *Suscriptores* salvo en los casos que así se establezca a través de convenios y/o contratos con el correspondiente consentimiento de los miembros integrantes de la *Comunidad Electrónica* o en los términos previstos en la *Ley de Emisión*.
127. La FNMT-RCM opera y mantiene sus capacidades de mantenimiento de sus CRL y servicio OCSP con recursos suficientes para proporcionar un tiempo de respuesta máximo de diez segundos bajo condiciones normales de operación.

6.2. CERTIFICADO DE COMPONENTE PARA EL SERVICIO FNMT DE SELLADO DE TIEMPO

128. Un caso específico de *Certificado de componente* es el que la FNMT-RCM utiliza para proveer uno de sus servicios de confianza: el *Servicio de Sellado de Tiempo*, de conformidad con la Declaración de Política y Prácticas de Sellado de Tiempo, que puede consultarse en <http://www.cert.fnmt.es/dpcs/>
129. El *Certificado* que utiliza la FNMT-RCM para crear los *Sellos de Tiempo electrónicos* mediante su *Servicio de Sellado de Tiempo* puede descargarse desde la sede electrónica <https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt>

7. TARIFAS

130. FNMT-RCM aplicará a las Administraciones Públicas las tarifas aprobadas por la Subsecretaría de la cual depende para la emisión de los *Certificados* o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizado para tal efecto.
131. Las tarifas a aplicar al sector privado se rigen por el contrato suscrito para la provisión de *Certificados*. Adicionalmente, la FNMT – RCM podrá establecer las tarifas y los medios de pago que considere oportunos en cada momento por la expedición de los *Certificados* a los *Suscriptores*. El precio y condiciones de pago de los *Certificados* podrán ser consultados en la página web de la FNMT – RCM o bien serán facilitados por el área comercial correspondiente bajo petición a la dirección de correo electrónico comercial.ceres@fnmt.es.

8. AUDITORÍAS

132. La Autoridad de Certificación “AC Componentes” está sujeta a auditorías periódicas, conforme con los requisitos establecidos por el estándar europeo ETSI EN 319 401 “General Policy Requirements for Trust Service Providers”.
133. La FNMT – RCM realiza autoevaluaciones, al menos trimestralmente, de un 20% de todos los *Certificados* emitidos durante el período que comienza inmediatamente después de la muestra de autoevaluación anterior.
134. El *Certificado de componente* de sello de entidad y el *Certificado de componente* como *Unidad de Sellado de Tiempo* del *Servicio cualificado de Sellado de Tiempo* de la FNMT – RCM, son *Certificados cualificados* de conformidad con el Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. Por tanto, las auditorías periódicas garantizan el cumplimiento de los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”, ETSI EN 319 412-3 “Certificate profile for certificates issued to legal persons” y ETSI EN 319 412-4 “Certificate profile for web site certificates”. Dichas auditorías son realizadas anualmente por una empresa externa acreditada.

9. PERFILES DE CERTIFICADOS

135. Todos los *Certificados* emitidos bajo esta política son de conformidad con el estándar X.509 versión 3. En la página <http://www.cert.fnmt.es/dpcs/> se puede consultar el perfil completo de cada *Certificado*.

9.1. RESTRICCIONES DE LOS NOMBRES

136. La codificación de los *Certificados* sigue el estándar RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. Todos los campos definidos en el perfil de los *Certificados* en el anexo II de las presentes *Políticas de*

Certificación, excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

9.2. USO DE LA EXTENSIÓN POLICY CONSTRAINTS

137. La extensión Policy Constraints del certificado raíz de la AC no es utilizado.

9.3. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

138. La extensión Certificate Policies incluye un campo de Policy Qualifier: CPS Pointer, que contiene la URL donde se publica la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y las *Políticas de Certificación y Prácticas de Certificación Particulares* aplicables a los *Certificados*.

9.4. TRATAMIENTO SEMÁNTICO DE LA EXTENSIÓN “CERTIFICATE POLICY”

139. La extensión Certificate Policy incluye el campo OID de política, que identifica la política asociada al *Certificado* por parte de la FNMT – RCM, así como los dos campos relacionados en el apartado anterior.

ANEXO I: IDENTIFICACIÓN DEL CERTIFICADO DE LA AUTORIDADES DE CERTIFICACIÓN

La Autoridad de Certificación implicada en el servicio utiliza para la firma / sello de *Certificados* y CRLs el *Certificado* identificado a continuación:

Certificado de la Autoridad de Certificación “AC Componentes Informáticos”

Nombre distintivo: OU = AC Componentes Informáticos, O = FNMT-RCM, C = ES

- Número de serie: 34:C6:AB:04:4E:36:99:12:51:C8:25:0B:6C:94:D6:C0
- Período de validez desde: jueves, 24 de junio de 2013
- Período de validez hasta: martes, 24 de junio de 2028
- Huellas digitales:
 - Huella digital (sha1):
C7:72:B4:8D:23:85:E5:02:E8:47:37:DB:E7:87:B6:43:11:91:12:47
 - Huella digital (sha256):
F0:38:42:1F:07:F2:0D:63:A2:0D:36:91:E5:A1:78:AB:84:59:EB:E5:70:C1:64:7B:
:76:90:55:4E:F2:38:76:AB