DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN DE CERTIFICADOS CUALIFICADOS DE SEDE ELECTRÓNICA

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	21/04/2021
Revisado por:	FNMT-RCM	26/04/2021
Aprobado por:	FNMT-RCM	28/04/2021

Versión	Fecha	Descripción
1.0	5/03/2019	Declaración de Prácticas y Políticas de Certificación de Certificados Cualificados de sede electrónica, bajo la jerarquía de la AC Raíz FNMT
1.1	30/05/2019	Actualización métodos de validación de dominios conforme a CA/Browser Forum Baseline Requeriments.
1.2	18/11/2019	Incorporación de referencia explícita al identificador de dominio a los efectos de las comprobaciones con el registro AAC
1.3	12/12/2019	Revisión general y actualización de mejora
1.4	01/10/2020	Incorporación del EKU "Autenticación de cliente" a los certificados de autenticación de sitios web
1.5	18/02/2021	Se incorpora dirección URL donde se publicó la lista de fuentes de consulta de Agencia de Registro
1.6	28/04/2021	Revisión anual y revisión Política Mozilla v.2.7.1 Se incluye información acerca de los métodos para comunicar un compromiso de claves

Referencia: DPC/DPCsede_0106/SGPSC/2021

Documento clasificado como: *Público*

Índice de contenidos

Índice de tablas

1. INTRODUCCIÓN

1. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, de aquí en adelante FNMT-RCM, con NIF Q2826004-J, es una entidad pública empresarial de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que, como organismo público, tiene personalidad jurídica pública diferenciada, patrimonio y tesorería propios, y autonomía de gestión en los términos de dicha ley.

2. Está adscrita al Ministerio de Hacienda, el cual, a través de la Subsecretaría de Hacienda, ejercerá la dirección estratégica y el control de eficacia de la Entidad en los términos previstos en la citada Ley 40/2015.

3. La FNMT-RCM cuenta con una larga trayectoria histórica en la realización de sus actividades industriales, así como el respaldo del Estado. Desde la entrada en vigor del artículo 81, de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social y sus modificaciones, ha contribuido a impulsar la extensión de los servicios a los que ha sido facultada y ha alcanzado un destacado puesto en la prestación de los servicios de confianza.

4. Asimismo, la FNMT-RCM, a través del Departamento CERES (CERtificación ESpañola), acredita ser un *Prestador Cualificado de Servicios de Confianza*, 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, a través de una entidad independiente y en el marco de un esquema de certificación, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

1.1. OBJETO

5. El presente documento tiene por objeto la información pública de las condiciones y características de los servicios de confianza dirigidos a los usuarios de los *Certificados de electrónica* por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo en concreto las obligaciones que se compromete a cumplir en relación con

   - la gestión de dichos *Certificados*, las condiciones aplicables a la solicitud, emisión, uso y extinción de la vigencia de los mismos, y
   - la prestación del servicio de consulta del estado de validez de los *Certificados*, así como las condiciones aplicables al uso del servicio y garantías ofrecidas.

6. Además, en el presente documento se recogen, bien directamente o con referencias a la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM* de la que depende la presente Declaración, los detalles del régimen de responsabilidad aplicable a las partes usuarias y/o que confían en los servicios mencionados en el párrafo anterior, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

7. El presente documento se denomina "*Declaración de Prácticas y Políticas de Certificación de certificados cualificados de sede electrónica*", y en adelante será citado en este documento y con el ámbito descrito en el mismo como "*Declaración de Prácticas y Políticas Particulares*" o por su acrónimo "*DPPP*".

8. Las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

9. En caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, tendrá preferencia lo aquí articulado.

10. La presente *Política de Certificación* tiene la siguiente identificación:

Tipo de política asociada: QCP-web. OID: 0.4.0.194112.1.4

Versión: 1.6

Fecha de expedición: 28/04/2021

Localización: http://www.cert.fnmt.es/dpcs/

DPC relacionada: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM

Localización: http://www.cert.fnmt.es/dpcs/

11. El *Certificado de autenticación de sitios web* es un tipo de certificado orientado a garantizar que el nombre del dominio del sitio web al que se conectan los usuarios de Internet es auténtico, mediante el uso de protocolos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (TLS/SSL). Cuando dicho sitio web es una *Sede electrónica,* a dicho *Certificado de autenticación de sitios web* se le denomina *Certificado de sede electrónica*.

12. En el ámbito de la presente *DPPP*, la FNMT-RCM expide los siguientes tipos de *Certificados de autenticación de sitios web*, con la consideración de cualificados[1], cuya descripción se encuentra en el apartado "1.6.1 Definiciones" del presente documento:

[1] Expedidos conforme a los requisitos establecidos en el anexo IV del 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.

Tipo de *Certificado*	Referencia / OID[2] de política
Certificado de Sede electrónica	1.3.6.1.4.1.5734.3.3.12.1

1.3. PARTES INTERVINIENTES

13. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *DPPP* son las siguientes:

1. Autoridad de Certificación
2. Autoridad de Registro
3. Suscriptores o titulares de los *Certificados*
4. Partes que confían
5. Otros participantes

1.3.1. Autoridad de Certificación

14. La FNMT-RCM es la *Autoridad de Certificación* que expide los Certificados electrónicos objeto de la presente *DPPP*. A estos efectos, existen las siguientes *Autoridades de Certificación*:

a) Autoridad de Certificación raíz. Dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas. El certificado raíz de esta AC viene identificado por la siguiente información:

Tabla 1 – Certificado de la AC RAIZ FNMT-RCM

Certificado de la AC RAIZ FNMT-RCM	
Sujeto	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES

[2] *Nota*: El OID o identificador de política es una referencia que se incluye en el *Certificado* al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.

Certificado de la AC RAIZ FNMT-RCM	
Número de serie (hex)	5D:93:8D:30:67:36:C8:06:1D:1A:C7:54:84:69:07
Validez	No antes: 29 de octubre de 2008. No después: 1 de enero de 2030
Longitud clave pública	RSA 4.096 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	F7 7D C5 FD C4 E8 9A 1B 77 64 A7 F5 1D A0 CC BF 87 60 9A 6D

b) Autoridades de Certificación subordinadas: expiden los *Certificados* de entidad final objeto de la presente *DPPP*. Los certificados de dichas Autoridades vienen identificados por la siguiente información:

Tabla 2 – Certificado de la AC subordinada "AC Administración Pública"

Certificado de la AC subordinada "AC Administración Pública"	
Sujeto	CN = AC Administración Pública, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	02
Validez	No antes: 21 de mayo de 2010. No después: 21 de mayo de 2022
Longitud clave pública	RSA 2.048 bits
Algoritmo de firma	RSA – SHA256
Identificador de clave	14 11 E2 B5 2B B9 8C 98 AD 68 D3 31 54 40 E4 58 5F 03 1B 7D

15. La Autoridad de Certificación subordinada "AC Administración Pública" expide, bajo las presentes DPPP, el *Certificado de Sede electrónica*.

1.3.2. Autoridad de Registro

16. La FNMT-RCM es la única *Autoridad de Registro* que actúa en el proceso de expedición de este tipo de *Certificados*. Realiza las tareas de identificación y comprobación, con el fin principal de garantizar que el *Certificado* se le expide al *Suscriptor* que tiene el control del nombre de dominio que se incorpora al *Certificado*.

1.3.3. Suscriptores de los certificados

17. Los *Suscriptores* son las personas jurídicas a quienes se expide este tipo de *Certificados* y que están legalmente obligados por un acuerdo que describe los términos de uso del *Certificado.*

18. En el caso de los *Certificados de sede electrónica,* el *Suscriptor* es siempre una administración pública, órgano, organismo público o entidad de derecho público, que tiene el control del nombre de dominio de la *Sede electrónica*.

1.3.4. Partes que confían

19. Las partes que confían son aquellos usuarios de Internet que establecen conexiones a sitios web mediante el uso de protocolos TLS/SSL que incorporan este tipo de *Certificados* y deciden confiar en ellos.

1.3.5. Otros participantes

20. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

21. Los *Certificados* expedidos bajo esta *Política de Certificación* se consideran válidos como medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad, la FNMT-RCM, auténtica y legítima, que respalda la existencia de dicho sitio web.

22. Adicionalmente, los *Certificados de sede electrónica* son un subconjunto de los *Certificados de autenticación de sitios web*, que se expiden como sistemas de identificación de una *Sede electrónica* que garantiza la comunicación segura con la misma, en los términos definidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

23. Todos los *Certificados* expedidos bajo la presente *Política de Certificación* son *Certificados Cualificados* conforme al 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 (Reglamento eIDAS) y de conformidad con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-4 "Certificate profile for web site certificates".

1.4.2. Restricciones en el uso de los certificados

24. Si una *Entidad usuaria* o un tercero desean confiar en estos *Certificados* sin acceder al *Servicio de información y consulta sobre el estado de validez de los certificados* expedidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas y Prácticas de Certificación Particulares*, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.

25. No se podrá emplear este tipo de *Certificados* para:

- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Firmar software o componentes.
- Generar *Sellos de tiempo* para procedimientos de *Fechado electrónico.*
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

26. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, con NIF Q2826004-J, es la *Autoridad de Certificación* que expide los certificados a los que aplica la presente *Declaración de Prácticas y Políticas de Certificación*.

1.5.2. Datos de contacto

27. La dirección de contacto de la FNMT-RCM como *Prestador de Servicios de Confianza* es la siguiente:

Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

Teléfono: 902 181 696

28. Para informar problemas de seguridad relacionados con un certificado, tales como sospecha de compromiso clave, uso indebido o fraude, envíenos un Informe de incidencia sobre certificado a la cuenta de correo electrónico: incidentes.ceres@fnmt.es.

1.5.3. Responsables de adecuación de la DPC

29. La Dirección de la FNMT-RCM dispone, dentro de sus competencias, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento, tanto para las Prácticas de Certificación Particulares, como para la Política de Certificación correspondiente.

1.5.4. Procedimiento de aprobación de la DPC

30. La FNMT-RCM gestiona sus servicios de certificación y emite certificados de conformidad con la última versión de 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/

31. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la presente 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.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

32. A los efectos de lo dispuesto en la presente *DPPP*, cuando los términos comiencen con letra mayúscula y estén en cursiva, se tendrán en cuenta de forma general las definiciones expresadas en la DGPC y, en particular, las expresadas a continuación:

- *Certificado de autenticación de sitios web:* Es un *Certificado* que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el *Certificado.*
- *Certificado de sede electrónica*: *Certificado de autenticación de sitios web* que identifica a una *Sede electrónica,* garantizando la comunicación segura con la misma en los términos definidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- *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.
- *Declaración de Prácticas de Certificación (DPC):* Declaración puesta a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita por parte de la FNMT-RCM. Tiene la consideración de documento de seguridad en el que se detallan, en el marco eIDAS, las obligaciones que los *Prestadores de Servicios de Confianza* se comprometen a cumplir en relación con la gestión de los *Datos de creación y verificación*

de firma y de los *Certificados electrónicos*, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los *Certificados*, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los *Certificados*.

- *Declaración de Prácticas y Políticas Particulares (DPPP): DPC* particular que aplica a la expedición de un conjunto determinado de *Certificados* expedidos por la FNMT-RCM bajo las condiciones particulares recogidas en dicha Declaración, y que le son de aplicación las Políticas particulares definidas en la misma.
- *Informe de incidencia con un certificado:* queja de sospecha de compromiso clave, mal uso del certificado u otros tipos de fraude, compromiso, mal uso o conducta inapropiada relacionada con los certificados
- *Organismo de supervisión:* organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el artículo 17 del Reglamento eIDAS. En España, actualmente es el Ministerio de Economía y Empresa.
- *Personal al servicio de la Administración Pública*: Funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público.
- *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 sitios web* para su nombre de dominio.
- *Responsable de Operaciones de Registro*: Persona física nombrada por el representante de la Administración pública, organismo público o entidad de derecho público, para tramitar las solicitudes de *Certificados* de *Sede electrónica*.
- *Representante del Suscriptor*: es la persona física representante legal, o persona autorizada por éste, de la organización *Suscriptora* del *Certificado de autenticación de sitios web*, para la solicitud y uso de dicho *Certificado*.
- *Sede electrónica*: Dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.
- *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. Bajo las presentas *Políticas de Certificación*, dicho servicio consiste en la expedición de *Certificados de autenticación de sitios web*. El *Suscriptor* se referencia en el campo *Sujeto* del *Certificado* y es el titular y responsable de su uso y posee el control exclusivo y la capacidad de decisión sobre el mismo.

(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)

1.6.2. Acrónimos

33. A los efectos de lo dispuesto en la presente *DPPP*, son de aplicación los siguientes acrónimos, cuyo significado es acorde con el estándar europeo ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

AC: Autoridad de Certificación

AR: Autoridad de Registro

ARL: Lista de Revocación de Autoridades de Certificación

CN: Nombre común (Common Name)

CRL: Lista de *Certificados* revocados

DN: Nombre distintivo (Distinguished Name)

DPC: Declaración de Prácticas de Certificación

eIDAS: Reglamento 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.

EV: Validación extendida (Extended Validation).

ETSI: European Telecommunications Standards Institute

HSM: Módulo de seguridad criptográfico (Hardware Security Module). Es un dispositivo de seguridad que genera y protege claves criptográficas.

OCSP: Protocolo de internet usado para obtener el estado de un certificado en línea (Online Certificate Status Protocol)

OID: Identificador de Objeto (Object IDentifier)

OV: Validación de Organización (Organizational Validation).

PDS: Declaración informativa de la PKI (PKI Disclosure Statement).

PIN: Número de identificación personal (Personal Identification Number).

PKCS: Estándares PKI desarrollados por Laboratorios RSA (Public Key Cryptography Standards).

TLS/SSL: Protocolos que proporcionan cifrado de datos y autenticación entre aplicaciones y servidores (Transport Layer Security/Secure Socket Layer protocol).

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIO

34. La FNMT-RCM, como como *Prestador de Servicios de Confianza*, mantiene un repositorio de información pública, disponible en horario 24x7, todos los días del año, con las características que se exponen en los siguientes apartados y con acceso a través de la dirección:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

35. La información relativa a la expedición de *Certificados* electrónicos objeto de la presente *DPPP,* accesible a través de la sede electrónica de la FNMT-RCM *(*https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion), incluye las siguientes informaciones:

- Declaraciones de prácticas y políticas de Certificación.
- Perfiles de los *Certificados* y de las *Listas de revocación*.
- Las declaraciones informativas de la PKI (PDS).
- Los términos y condiciones de uso de los *Certificados*, como instrumento jurídico vinculante.

36. Adicionalmente, se puede acceder a la descarga de los Certificados raíz y de AC subordinadas de la FNMT-RCM, así como a información adicional, a través de la dirección:

https://www.sede.fnmt.gob.es/descargas/

2.3. FRECUENCIA DE PUBLICACIÓN

37. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la presente *DPPP*, siguiendo las pautas establecidas en el apartado "1.5.4. Procedimiento de aprobación de la DPC" del presente documento de *DPPP*.

38. Cualquier modificación en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* o en las *Políticas* y *Prácticas de Certificación Particulares* será publicada de forma inmediata en la URL de acceso a las mismas.

39. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Frecuencia de generación de CRLs", de la *DGPC*.

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

40. Todos los repositorios anteriormente citados son de acceso libre para la consulta y, en su caso, descarga de la información. Así mismo, la FNMT-RCM ha establecido controles para impedir que personas no autorizadas puedan añadir, modificar o borrar información incluida en sus repositorios y para proteger la autenticidad e integridad de dicha información.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. DENOMINACIÓN

41. La codificación de los *Certificados* sigue el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de los *Certificados* en las *Políticas de Certificación* y *Prácticas de Certificación Particulares,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

3.1.1. Tipos de nombres

42. Los *Certificados* electrónicos de entidad final objeto de la presente *DPPP* contienen un nombre distintivo (*DN*) en el campo Subject Name, que se componen según se describe en la información relativa al perfil del Certificado (apartado 7.1 del presente documento).

3.1.2. Significado de los nombres

43. Todos los nombres distintivos (*DN*) del campo Subject Name son significativos. La descripción de los atributos asociados al *Suscriptor* del *Certificado* es legible por humanos (véase el apartado 7.1.4 Formato de nombres del presente documento).

3.1.3. Seudónimos

44. Bajo la presente *Política de Certificación* la FNMT – RCM no admite el uso de seudónimos.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

45. Se aplican los requisitos definidos por el estándar X.500 de referencia en la norma ISO/IEC 9594.

3.1.5. Unicidad de los nombres

46. El nombre distintivo (*DN*) asignado al *Suscriptor* del *Certificado* dentro del dominio del *Prestador de Servicios de Confianza* será único.

3.1.6. Reconocimiento y autenticación de marcas registradas

47. Los suscriptores no podrán solicitar *Certificados* con ningún contenido que infrinja los derechos de propiedad intelectual de un tercero. Véase el apartado correspondiente en la *DGPC*.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

48. La FNMT-RCM realiza el proceso de validación de la información incluida en el *Certificado de autenticación de sitios web* 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 dirección https://cabforum.org/baseline-requirements-documents/ y de conformidad con la última versión de los requisitos definidos por la entidad CA/Browser forum en su “guía para la expedición y gestión de Certificados de Validación Extendida” (que pueden consultarse en la dirección https://cabforum.org/extended-validation/).

3.2.1. Métodos para probar la posesión de la clave privada

49. La FNMT-RCM recibe una solicitud de *Certificado*, en formato PKCS#10, firmada digitalmente por la *Clave privada* generada por el *Representante del Suscriptor* en su entorno. Antes de proceder a la expedición del *Certificado*, la FNMT-RCM verifica dicha firma, garantizando que la *Clave pública* incluida en la solicitud se corresponde con la *Clave privada* generada por el *Responsable del Certificado*.

3.2.2. Autenticación de la identidad de la Organización

3.2.2.1 Identidad

50. La FNMT-RCM verifica la existencia legal, la dirección y la identidad de la organización suscriptora del *Certificado* mediante diferentes métodos, en función del tipo de organización (privada, pública o de negocio).

51. En todos los casos, los *Suscriptores* de los *Certificados* expedidos bajo las presentes DPPP son siempre entidades públicas españolas. Por tanto, la verificación de su existencia, de estar legalmente reconocida, activa en el momento de expedición del *Certificado* e inscrita formalmente, se realizará mediante consulta directa de la AR de la FNMT-RCM al inventario de entes del sector público de la Intervención General de la Administración del Estado, dependiente del Ministerio de Hacienda, o al inventario de la Agencia Estatal de Administración Tributaria.

52. La lista de las fuentes de consulta de Agencias de Registro es publicada en la web de la FNMT-RCM (https://www.cert.fnmt.es/registro/utilidades)

53. La FNMT-RCM no expide *Certificados de autenticación de sitios web* cuyo *Suscriptor* sea una persona física.

54. La FNMT-RCM verifica que el nombre y número de identificación fiscal de la organización suscriptora del *Certificado* incorporados a la solicitud del mismo coinciden con el nombre y número de identificación fiscal inscritos formalmente en los registros consultados según se describe en los apartados anteriores.

3.2.2.2 Nombre comercial o marca registrada

55. Si la información de la identidad del sujeto incluye un nombre comercial o marca registrada, el FNMT-RCM utilizará los mismos procedimientos y criterios de verificación que en la Sección 3.2.2.1 para verificar el derecho del Solicitante a usar el nombre comercial o marca registrada.

3.2.2.3 Verificación del país

56. Todos los *Certificados* expedidos bajo las presentes DPPP son emitidos a Suscriptores que son entidades públicas españolas. El país se verificará utilizando cualquiera de los métodos indicados en la Sección 3.2.2.1

3.2.2.4 Validación de la autorización y control sobre el dominio

57. Para validar el dominio de los Certificados de autenticación de sitios 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", "3.2.2.4.4 Constructed Email to Domain Contact" o "3.2.2.4.7 DNS Change ".

58. La FNMT-RCM confirma que el Representante del Suscriptor 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 Representante del Suscriptor 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.

59. 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 púbicos 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).

3.2.2.5 Autenticación para una dirección IP

60. Bajo la presente *DPPP,* no se emiten certificados para identificar direcciones IP.

3.2.2.6 Validación de dominio wildcard

61. Bajo la presente *DPPP* no se emiten certificados con dominios wildcard.

3.2.2.7 Fiabilidad de las fuentes de datos

62. Antes de utilizar cualquier fuente de datos como fuente de datos confiable, la *RA* evaluará la fuente en cuanto a su confiabilidad, precisión y resistencia a la alteración o falsificación.

3.2.2.8 Registro ACC

63. La FNMT-RCM comprueba si hay un Registro AAC para cada nombre de dominio que incluye en un Certificado de autenticación de sitios 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. El identificador de dominio reconocido como propio asociado a la autoridad de certificación de la FNMT se ha establecido en "fnmt.es".

3.2.3. Autenticación de la identidad de la persona física solicitante

64. La AR de la FNMT-RCM comprueba que el *Representante del Suscriptor* coincide con la persona física que solicita un *Certificado de autenticación de sitios web*, mediante la firma electrónica de un formulario de solicitud. El uso de un *Certificado* cualificado de firma electrónica garantiza la autenticidad de su identidad.

3.2.4. Información no verificada del Suscriptor

65. Toda la información incorporada al *Certificado* electrónico es verificada por la *Autoridad de Registro*, por tanto, no se incluye información no verificada en el campo "Subject" de los certificados expedidos.

3.2.5. Validación de la capacidad de representación

66. La AR de la FNMT-RCM verifica que el *Solicitante* tiene suficiente capacidad de representación mediante la firma electrónica del formulario de solicitud, según se describe en el apartado 3.2.3 de la presente DPPP, aceptando el uso de un *Certificado* cualificado, acreditando adicionalmente que posee suficiente capacidad de representación para realizar la solicitud del *Certificado*.

67. La validez de las evidencias obtenidas como resultado de las consultas realizadas para la autenticación de la identidad de la Organización y/o la autenticación de la identidad de la persona física solicitante, conforme a los apartados 3.2.2 y 3.2.3 del presente documento, será, como máximo, el de vigencia del *Certificado* a expedir. Por tanto, si hubiera un *Certificado* activo y se está solicitando la expedición de otro *Certificado* del mismo tipo y para el mismo *Suscriptor* y nombre/s de dominio/s, no será necesario recabar de nuevo las citadas evidencias de identificación de la organización suscriptora del *Certificado* y/o de la identidad de la persona física solicitante. A estos efectos, se recuerda que el periodo máximo de vigencia de los *Certificados* expedidos bajo las presentes políticas es de 1 año.

3.2.6. Criterios de interoperación

68. No existen relaciones de interactividad con Autoridades de Certificación externas a FNMT-RCM.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

3.3.1. Identificación y autenticación para renovación rutinaria de claves

69. Los Suscriptores de los Certificados deberían solicitar la renovación de los mismos antes de que expire su período de vigencia. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado de esta *DPPP* correspondiente al proceso de renovación de *Certificados* (véase apartado 4.6 del presente documento).

3.3.2. Identificación y autenticación para renovación de claves después de una revocación

70. La FNMT-RCM no renueva *Certificados* que han sido revocados. El proceso de renovación del *Certificado* tras la revocación del mismo será el mismo que el que se sigue en la emisión inicial de dicho *Certificado*.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

71. Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado de esta *DPPP* correspondiente al proceso de revocación de *Certificados* (véase apartado 4.9 del presente documento).

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

72. Únicamente podrán solicitar *Certificados de autenticación de sitio web* los *Representantes del Suscriptor,* o personas debidamente autorizados a solicitar el *Certificado* en nombre del *Suscriptor*, que hayan acreditado tener el control sobre el nombre del dominio a incluir en el *Certificado*. El citado control sobre el nombre del dominio será verificado por la FNMT-RCM según se describe en el apartado "3.2 Validación inicial de la identidad" de la presente *DPPP*.

4.1.2. Proceso de registro y responsabilidades

73. Cada Solicitante deberá presentar una solicitud de Certificado y la información requerida antes de emitir un Certificado. El FNMT-RCM autentica y protege todas las comunicaciones frente a modificaciones con el Solicitante.

74. El proceso de registro incluye las siguientes fases:

- Enviar una solicitud de Certificado completa y aceptar los términos y condiciones aplicables. Con esta aceptación, los Suscriptores garantizan que toda la información contenida en la solicitud de Certificado es correcta.
- Generar un par de claves,
- Entregar la clave pública del par de claves a la CA y
- Pagar cuando proceda las tarifas aplicables.

75. La AR de la FNMT-RCM realiza la verificación de la identidad de la Organización suscriptora y del *Representante del Suscriptor*, y comprueba que la solicitud del *Certificado* es correcta completa y debidamente autorizada, de conformidad con los requisitos definidos en el apartado "3.2 Validación inicial de la identidad" del presente documento. FNMT-RCM podrá realizar comprobaciones adicionales a los procesos de validación descritos en el citado apartado.

76. FNMT-RCM recopilará las evidencias correspondientes a las comprobaciones realizadas y quedarán almacenadas en un repositorio.

77. El apartado 9.8 "Obligaciones y garantías" del presente documento establece las responsabilidades de las partes en este proceso.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

78. El *Representante del Suscriptor* remite a la AR de la FNMT-RCM un formulario, firmado electrónicamente con un *Certificado* electrónico cualificado, que recoge toda la información a incorporar en el *Certificado de autenticación de sitio web*. A partir de dicha información, la AR de la FNMT-RCM lleva a cabo las comprobaciones descritas en el apartado "3.2 Validación inicial de la identidad" de la presente *DPPP*.

79. 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.

80. La firma electrónica generada para la suscripción del contrato será verificada por la FNMT-RCM.

81. El empleo de los datos o la documentación de validación previa, obtenidos de una fuente de las especificadas en la sección 3.2, no se puede utilizar más de 12 meses después de que se validasen dichos datos o documentación

4.2.2. Aprobación o rechazo de la solicitud del certificado

82. La AR que actúa en el proceso de expedición de *Certificados de autenticación de sitios web* es siempre la propia FNMT-RCM y, por tanto, no delega la validación de dominios a ninguna otra AR.

83. La AR de la FNMT-RM realiza las comprobaciones relativas a la prueba de posesión de la *Clave privada* por parte del *Representante del Suscriptor*, la autenticación de la identidad de la Organización y de la persona que solicita el *Certificado*, así como la validación del dominio, según se describe en el apartado "3.2 Validación inicial de la identidad" de la presente *DPPP*, que darán como resultado la aprobación o el rechazo de la solicitud del mismo.

84. 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.

85. 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.

86. Si alguna de estas validaciones no ha podido ser confirmada, la FNMT-RCM rechazará la solicitud del *Certificado*, reservándose el derecho de no revelar los motivos de dicha

denegación. El *Representante del Suscriptor* cuya solicitud haya sido rechazada podrá volver a solicitarlo posteriormente.

87. El sistema de aprobación de expedición de *Certificados de autenticación de sitios web* requiere de la acción de al menos dos personas pertenecientes a la AR de la FNMT-RCM y autorizadas para este fin.

88. Adicionalmente, la FNMT-RCM comprueba si hay un *Registro AAC* para cada nombre de dominio que incluye en un *Certificado de autenticación de sitios 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. El identificador de dominio reconocido como propio asociado a la autoridad de certificación de la FNMT se ha establecido en "fnmt.es".

4.2.3. Tiempo en procesar la solicitud

89. El plazo de tiempo en procesar la solicitud de un *Certificado* depende en gran medida de que el *Representante del Suscriptor* proporcione la información y la documentación necesarias de la forma prevista en los procedimientos aprobados por la FNMT-RCM para este fin. No obstante, esta Entidad hará el esfuerzo necesario para que el proceso de validación que dará como resultado la aceptación o el rechazo de la solicitud no exceda de dos (2) días hábiles.

90. Este periodo de tiempo podrá, ocasionalmente, ser superado por motivos fuera del control de la FNMT-RCM. En estos casos, hará lo posible por mantener informado al *Representante del Suscriptor* que realizó la solicitud de las causas de tales retrasos.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

91. Una vez aprobada la solicitud del *Certificado* por parte de la AR de la FNMT-RCM, el sistema realiza algunas comprobaciones, como el tamaño de la *Clave pública* generada, y procede a expedir el *Certificado* conforme al perfil aprobado para cada tipo de *Certificado*.

92. Los procesos relativos a la emisión de *Certificados* electrónicos garantizan que todas las cuentas que intervienen en los mismos tienen autenticación multi-factor.

4.3.2. Notificación de emisión de certificado

93. Una vez emitido el *Certificado*, FNMT-RCM envía una comunicación a la dirección de correo electrónico consignada en el formulario de solicitud firmado por el *Representante del Suscriptor*, informando que está disponible dicho *Certificado* para su descarga.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

94. En el proceso de solicitud del *Certificado*, el *Representante del Suscriptor* acepta las condiciones de uso y expresa su voluntad de obtener el *Certificado*, como requisitos necesarios para la generación del mismo.

4.4.2. Publicación del certificado por la AC

95. Los *Certificados* generados son almacenados en un repositorio seguro de la FNMT-RCM.

4.4.3. Notificación de la emisión a otras entidades

96. Antes de la expedición de *Certificados de autenticación de sitio web* se envía un pre-certificado a los registros del servicio *Certificate Transparency* de aquellos proveedores con los que la FNMT-RCM mantiene un acuerdo para tal fin.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada del suscriptor y uso del certificado

97. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*. Corresponde la condición de custodio y el control de las claves del *Certificado* al *Responsable de Operaciones de Registro*. Por tanto, la *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad de dicho custodio y actuará como representante de la Entidad que tiene la titularidad, gestión y administración de la dirección electrónica correspondiente.

4.5.2. Uso del certificado y la clave pública por terceros que confían

98. Las entidades usuarias y terceros que confían utilizarán software que sea compatible con los estándares aplicables al uso de *Certificados* electrónicos (X.509, IETF, RFCs…). Si la conexión al sitio web requiriese de adicionales medidas de aseguramiento, dichas medidas han de ser obtenidas por las entidades usuarias.

99. Los terceros que confían en el establecimiento de una conexión segura garantizada por un *Certificado de autenticación de sitios web* deben cerciorarse de que dicha conexión fue creada durante el periodo de validez del *Certificado*, que dicho *Certificado* está siendo usado con el propósito para el que se expidió de acuerdo con la presente *DPPP*, así como verificar que en ese momento el *Certificado* está activo, mediante la comprobación de su estado de revocación en la forma y condiciones que se expresan en el apartado “4.10 Servicios de información del estado de los certificados” del presente documento.

4.6. RENOVACIÓN DEL CERTIFICADO

100. La renovación de un *Certificado* consiste en la emisión de un nuevo *Certificado* sin cambiar ninguna información del *Firmante*, *Clave pública* o cualquier otra información que aparezca

en el mismo. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

101. La FNMT no realiza renovaciones de *Certificados de sede electrónica*. La renovación con regeneración de claves de los *Certificados de autenticación de sitios web* se realiza siempre emitiendo nuevas claves públicas y privadas, siguiendo el mismo proceso que el descrito para la emisión de un *Certificado* nuevo

4.8. MODIFICACIÓN DEL CERTIFICADO

102. No es posible realizar modificaciones de los *Certificados* expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo *Certificado*.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

103. Los *Certificados de autenticación de sitios web* emitidos 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.

104. 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 su *Servicio de información y consulta sobre el estado de los certificados*.

105. 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.

106. 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 tiene el control del nombre de dominio del sitio web incluido en el *Certificado* no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o *Sedes electrónicas* que se desean proteger con tales *Certificados*, o su uso se

presta a engaño o confusión sobre la titularidad de tales aplicaciones, sitios web o *Sedes electrónicas* y, por tanto, de sus contenidos. 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:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) 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

d) La protección de la juventud y de la infancia.

107. La FNMT–RCM, se mantendrá indemne por parte de los titulares o responsables de los equipos, aplicaciones, sitios web o *Sedes electrónicas* que incumplan lo previsto en este apartado y que tengan relación con el *Certificado*, quedando exonerada de cualquier reclamación o reivindicación por el uso inadecuado de tales *Certificados*.

4.9.1. Circunstancias para la revocación

4.9.1.1 Causas de revocación de un Certificado de entidad final

108. Adicionalmente a lo previsto en el apartado anterior, en relación con la solicitud de un *Certificado* existiendo otro en vigor a favor del mismo dominio y mismo *Suscriptor*, serán causas de revocación de un *Certificado de autenticación de sitios web*:

a) La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de la *Clave Privada* asociada al *Certificado*.
- La violación o puesta en peligro del secreto de la *Clave Privada* asociada al *Certificado*.
- La no aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción, disolución o cierre del sitio web identificado por el *Certificado*.

d) Extinción o disolución de la personalidad jurídica del *Suscriptor*.

e) Terminación de la forma de representación del representante del *Suscriptor* del *Certificado.*

f) Incapacidad sobrevenida, total o parcial, del representante del *Suscriptor*.

g) Inexactitudes en los datos aportados por el *Representante del Suscriptor* para la obtención del *Certificado*, o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado*, de manera que éste ya no fuera conforme a la realidad.

h) Contravención de una obligación sustancial de esta *Declaración de Prácticas de Certificación* por parte del *Suscriptor*, del *Representante del Suscriptor* o de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*.

i) 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.

j) Resolución del contrato suscrito entre el *Suscriptor* o su *Representante*, y la FNMT-RCM, o el impago de los servicios prestados.

k) Violación o puesta en peligro del secreto de los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM, con los que firma / sella los *Certificados* que emite.

l) Incumplimiento de los requisitos definidos por los esquemas de auditorías a los que se somete la *Autoridad de Certificación* que expide los *Certificados* cubiertos por la presente *DPPP*, 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*.

109. En ningún caso se debe entender que la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a i) del presente apartado.

110. 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 *Representante del Suscriptor* siguiendo el procedimiento establecido para este tipo de *Certificados.*
- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*.
- 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 g) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.

111. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o el *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.

4.9.1.1 Causas de revocación de un Certificado de CA subordinada

112. La CA emisora revocará el certificado de la CA subordinada en el plazo de 7 días si en cualquiera de las siguientes situaciones:

a) La CA subordinada solicita la revocación por escrito;

b) La CA subordinada notifica a la CA emisora que la solicitud de certificado original no fue autorizada y no otorga autorización retroactivamente;

c) La CA emisora obtiene evidencia de que la Clave privada de la CA subordinada correspondiente a la Clave pública en el Certificado sufrió un Compromiso clave o ya no cumple con los requisitos de las secciones 6.1.5 y 6.1.6,

d) La CA emisora obtiene evidencia de que el *Certificado* fue mal utilizado;

e) La CA emisora es consciente de que el *Certificado* no se emitió de acuerdo con o que la CA subordinada no ha cumplido con los requisitos establecidos por la entidad CA/Browser fórum para este tipo de *Certificados*, las directrices de EV, o esta *DPPP*;

f) La CA emisora determina que cualquiera de la información que aparece en el Certificado es inexacta o engañosa;

g) La CA emisora o CA subordinada cesa sus operaciones por cualquier motivo y no ha hecho arreglos para que otra CA brinde apoyo de revocación para el Certificado;

h) El derecho de la CA emisora o de la CA subordinada a emitir Certificados según los requisitos establecidos por la entidad CA/Browser fórum vence o se revoca o finaliza, a menos que la CA emisora haya hecho arreglos para continuar manteniendo el repositorio de CRL / OCSP; o

i) La *DPPP* de la CA emisora requiere la revocación.

4.9.2. Quién puede solicitar la revocación

113. La CA, la RA y los Suscriptor puede iniciar la revocación de un certificado

114. La FNMT-RCM presumirá la competencia y capacidad del *Solicitante* de la revocación cuando se trate del *Responsable de Operaciones de Registro* correspondiente. Adicionalmente, estarán legitimados para solicitar la revocación de dicho *Certificado*:

- El órgano directivo, organismo o entidad pública *Suscriptora* del *Certificado* o persona en quien delegue.
- La *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad de derecho público, *Suscriptora* del *Certificado* a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*
    - es incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado,* o

- la persona física, custodio del *Certificado,* no se corresponda con el responsable máximo o designado para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación

siempre en el marco de los términos y condiciones aplicables a la revocación de este tipo de *Certificados*.

115. Adicionalmente, los suscriptores, las partes confiables, los proveedores de software de aplicaciones y otros terceros pueden informar a la CA emisora de una causa razonable para revocar el certificado, enviando un Informe de incidencia con un certificado

116. No obstante, la FNMT-RCM podrá revocar de oficio los *Certificados de autenticación de sitios web* en los supuestos recogidos en la presente *Declaración de Prácticas y Políticas de Certificación*.

4.9.3. Procedimiento de solicitud de la revocación

117. 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 de *Certificados de autenticación de sitios web*. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.

118. Adicionalmente, la FNMT-RCM revocará los *Certificados de sede electrónica* cuando la solicitud de revocación provenga de una *Oficina de Registro* designada por la Administración, cuyo procedimiento es el siguiente:

1. Personación del *Solicitante* ante una *Oficina de Registro*.

   Para revocar el *Certificado*, el *Solicitante* con capacidad y competencia suficientes, se personará ante una *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad *Suscriptora* del *Certificado* a revocar o será realizada directamente por el *Responsable de Operaciones de Registro*.

2. Comparecencia y documentación.

   El *Solicitante* aportará los datos que se le requieran y que acrediten:

   - su identidad personal,
   - su condición de *Personal al servicio de la Administración Pública, Suscriptora* del *Certificado* y titular de la dirección electrónica a través de la que se accede a la *Sede electrónica* objeto del *Certificado* o su condición de *Responsable de Operaciones de Registro*.
   - su condición de persona designada para la gestión de la dirección electrónica a través de la que se accede a la *Sede electrónica* objeto del *Certificado* a revocar o de personal adscrito a la *Oficina de Registro* designada a tal efecto por el organismo o entidad *Suscriptora* del *Certificado* a revocar.

   En el caso de que no se acrediten los puntos anteriores, la *Oficina de Registro* no procederá con la solicitud de revocación del *Certificado.*

3. Envío de la solicitud de revocación a la FNMT-RCM y tramitación.

Sin que existan causas notorias de falta de competencia del *Responsable de Operaciones de Registro* y/o una vez confirmada la identidad del *Solicitante*, vigencia de las condiciones exigidas a éste y suscrito el documento de solicitud de revocación, la *Oficina de Registro* procederá a validar los datos y a enviarlos a la FNMT-RCM para la revocación efectiva del *Certificado*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

Dicho envío sólo se producirá si la *Oficina de Registro* tiene potestad para actuar como tal en nombre del órgano, organismo o entidad de la Administración Pública *Suscriptora* del *Certificado* y si éste es titular de la dirección electrónica a través de la que se accede a la *Sede electrónica* objeto del *Certificado.*

Esta transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

119. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado de autenticación de sitios web*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados,* conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y la causa de revocación. El *Representante del Suscriptor* recibirá, a través de la dirección de correo electrónico consignada en la solicitud, la notificación del cambio de estado de vigencia del *Certificado*.

4.9.4. Periodo de gracia de la solicitud de revocación

120. No existe periodo de gracia asociado a este proceso, pues la revocación se realiza de forma inmediata a la recepción verificada de la solicitud de revocación.

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

121. Todas las solicitudes de revocación de certificados de entidad final, son procesadas en el plazo máximo de 24 horas desde la recepción de la misma.

122. La FNMT – RCM procede a la revocación inmediata del *Certificado de autenticación de sitios web* en el momento de realizar las comprobaciones descritas anteriormente o, en su caso, una vez comprobada la veracidad de la solicitud realizada mediante resolución judicial o administrativa.

4.9.6. Obligación de verificar las revocaciones por las partes que confían

123. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar:

- la *Firma Electrónica Avanzada* o el *Sello Electrónico Avanzado* del *Prestador de Servicios de Confianza* emisor del *Certificado,*
- que el *Certificado* continúa vigente y activo, y
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

4.9.7. Frecuencia de generación de CRLs

124. Las *Listas de Revocación* (*CRL*) de los certificados de entidad final se emiten al menos cada 12 horas, o cuando se produce una revocación y tienen un periodo de validez de 24 horas. Las *CRL* de los certificados de *Autoridad* se emiten cada 6 meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de 6 meses.

4.9.8. Periodo máximo de latencia de las CRLs

125. La publicación de las *Listas de Revocación* se realiza en el momento de generación de dichas Listas, por lo que el periodo de latencia entre la generación de la CRL y su publicación es nulo.

4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados

126. La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema se pondrá en marcha el Plan de continuidad de negocio para solventar el incidente a la mayor brevedad posible.

4.9.10. Requisitos de comprobación en línea de la revocación

127. La comprobación en línea del estado de revocación del *Certificado de autenticación de sitios web* puede realizarse mediante el *Servicio de información del estado de los certificados*, ofrecido a través de OCSP según se describe en el apartado 4.10 del presente documento. El interesado en utilizar dicho servicio deberá:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del certificado.
- Comprobar que la respuesta OCSP está firmada / sellada.

4.9.11. Otras formas de aviso de revocación disponibles

128. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

129. Véase el apartado correspondiente en la DGPC.

4.9.13. Circunstancias para la suspensión

130. No se contempla la suspensión de certificados.

4.9.14. Quién puede solicitar la suspensión

131. No se contempla la suspensión de certificados.

4.9.15. Procedimiento para la petición de la suspensión

132. No se contempla la suspensión de certificados.

4.9.16. Límites sobre el periodo de suspensión

133. No se contempla la suspensión de certificados.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

134. El funcionamiento del *Servicio de información y consulta del estado de los certificados* es el siguiente: el servidor OCSP recibe la petición OCSP efectuada por un *Cliente OCSP* y comprueba el estado de vigencia de los *Certificados* incluidos en la misma. En 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. Dicha respuesta es firmada / sellada con los *Datos de Creación de Firma* / *Sello* de la FNMT-RCM garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

135. Será responsabilidad de la Entidad usuaria contar con un *Cliente OCSP* para operar con el servidor OCSP puesto a disposición por la FNMT-RCM.

136. 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.

4.10.1. Características operativas

137. La información relativa a la validación de los *Certificados* electrónicos objeto de la presente *DPPP* es accesible a través de los medios descritos en la *DGPC*.

4.10.2. Disponibilidad del servicio

138. La FNMT-RCM garantiza el acceso a este servicio, en horario 24x7, por parte de los usuarios, titulares y las partes que confían en los *Certificados*, de forma segura, rápida y gratuita.

139. En el caso de indisponibilidad del servicio por operaciones de mantenimiento, la FNMT-RCM notificará esta 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.

4.10.3. Características opcionales

140. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

141. La suscripción finalizará en el momento de extinción de la vigencia del *Certificado de autenticación de sitios web*, ya sea por expiración del periodo de vigencia o por revocación del mismo.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

142. La FNMT-RCM no genera las *Claves privadas* de los *Certificados de autenticación de sitios web* y, por tanto, no las custodia ni puede recuperarlas.

4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión

143. No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DE PERSONAL

144. Véase el apartado correspondiente en la DGPC.

5.1. CONTROLES DE SEGURIDAD FÍSICA

145. Véase el apartado correspondiente en la DGPC.

5.1.1. Ubicación de las instalaciones

146. Véase el apartado correspondiente en la DGPC.

5.1.2. Acceso Físico

147. Véase el apartado correspondiente en la DGPC.

5.1.3. Electricidad y Aire Acondicionado

148. Véase el apartado correspondiente en la DGPC.

5.1.4. Exposición al agua

149. Véase el apartado correspondiente en la DGPC.

5.1.5. Prevención y Protección contra incendios

150. Véase el apartado correspondiente en la DGPC.

5.1.6. Almacenamiento de Soportes

151. Véase el apartado correspondiente en la DGPC.

5.1.7. Eliminación de Residuos

152. Véase el apartado correspondiente en la DGPC.

5.1.8. Copias de Seguridad fuera de las instalaciones

153. Véase el apartado correspondiente en la DGPC.

5.2. CONTROLES DE PROCEDIMIENTO

154. Véase el apartado correspondiente en la DGPC.

5.2.1. Roles de Confianza

155. Véase el apartado correspondiente en la DGPC.

5.2.2. Número de personas por tarea

156. Véase el apartado correspondiente en la DGPC.

5.2.3. Identificación y autenticación para cada rol

157. Véase el apartado correspondiente en la DGPC.

5.2.4. Roles que requieren segregación de funciones

158. Véase el apartado correspondiente en la DGPC.

5.3. CONTROLES DE PERSONAL

159. Véase el apartado correspondiente en la DGPC.

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

160. Véase el apartado correspondiente en la DGPC

5.3.2. Procedimientos de verificación de antecedentes

161. Véase el apartado correspondiente en la DGPC

5.3.3. Requisitos de formación

162. Véase el apartado correspondiente en la DGPC

5.3.4. Requisitos y frecuencia de actuación formativa

163. Véase el apartado correspondiente en la DGPC

5.3.5. Secuencia y frecuencia de rotación laboral

164. Véase el apartado correspondiente en la DGPC

5.3.6. Sanciones por acciones no autorizadas

165. Véase el apartado correspondiente en la DGPC

5.3.7. Requisitos de contratación de personal

166. Véase el apartado correspondiente en la DGPC

5.3.8. Suministro de documentación al personal

167. Véase el apartado correspondiente en la DGPC

5.4. PROCEDIMIENTOS DE AUDITORÍA

168. Véase el apartado correspondiente en la DGPC.

5.4.1. Tipos de eventos registrados

169. Véase el apartado correspondiente en la DGPC.

5.4.2. Frecuencia de procesamiento de registros

170. Véase el apartado correspondiente en la DGPC.

5.4.3. Periodo de conservación de los registros

171. Véase el apartado correspondiente en la DGPC.

5.4.4. Protección de los registros

172. Véase el apartado correspondiente en la DGPC.

5.4.5. Procedimientos de copias de seguridad de los registros auditados

173. Véase el apartado correspondiente en la DGPC.

5.4.6. Sistemas de recolección de registros

174. Véase el apartado correspondiente en la DGPC.

5.4.7. Notificación al sujeto causante de los eventos

175. Véase el apartado correspondiente en la DGPC.

5.4.8. Análisis de vulnerabilidades

176. Véase el apartado correspondiente en la DGPC.

5.5. ARCHIVADO DE REGISTROS

177. Véase el apartado correspondiente en la DGPC.

5.5.1. Tipos de registros archivados

178. Véase el apartado correspondiente en la DGPC.

5.5.2. Periodo de retención del archivo

179. Véase el apartado correspondiente en la DGPC.

5.5.3. Protección del archivo

180. Véase el apartado correspondiente en la DGPC.

5.5.4. Procedimientos de copia de respaldo del archivo

181. Véase el apartado correspondiente en la DGPC.

5.5.5. Requisitos para el sellado de tiempo de los registros of Records

182. Véase el apartado correspondiente en la DGPC.

5.5.6. Sistema de archivo

183. Véase el apartado correspondiente en la DGPC.

5.5.7. Procedimientos para obtener y verificar la información archivada

184. Véase el apartado correspondiente en la DGPC.

5.6. CAMBIO DE CLAVES DE LA AC

185. Véase el apartado correspondiente en la DGPC.

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

186. Véase el apartado correspondiente en la DGPC.

5.7.1. Gestión de incidentes y vulnerabilidades

187. Véase el apartado correspondiente en la DGPC.

5.7.2. Actuación ante datos y software corruptos

188. Véase el apartado correspondiente en la DGPC.

5.7.3. Procedimiento ante compromiso de la clave privada de la AC

189. Véase el apartado correspondiente en la DGPC.

5.7.4. Continuidad de negocio después de un desastre

190. Véase el apartado correspondiente en la DGPC.

5.8. CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CONFIANZA

191. Véase el apartado correspondiente en la DGPC.

6. CONTROLES DE SEGURIDAD TÉCNICA

192. Véase el apartado correspondiente en la DGPC.

6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES

6.1.1. Generación del par de claves

6.1.1.1 Generación del par de Claves de la CA

193. En relación con la información de las *Claves* que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Confianza,* véase el apartado correspondiente en la *DGPC*.

6.1.1.2 Generación del par de Claves de la RA

194. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

195. Las *Claves privadas* de los *Certificados de autenticación de sitios web* son generadas y custodiadas por el *Suscriptor* del *Certificado*.

6.1.2. Envío de la clave privada al suscriptor

196. No existe ninguna generación ni entrega de la *Clave privada* al *Titular* por parte de la *CA*.

6.1.3. Envío de la clave pública al emisor del certificado

197. La *Clave pública,* generada junto a la *Clave privada* sobre el dispositivo de generación y custodia de claves, es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

6.1.4. Distribución de la clave pública de la AC a las partes que confían

198. La FNMT-RCM distribuye las *Claves públicas,* tanto de la AC raíz como de las AC Subordinadas que expiden los *Certificados de autenticación de sitios web,* a través de varios medios, como son mediante publicación en su sede electrónica (www.sede.fnmt.gob.es) o mediante información pública a través del presente documento, en el apartado "1.3.1. Autoridad de Certificación".

6.1.5. Tamaños de claves y algoritmos utilizados

199. El algoritmo y el tamaño de claves utilizados son los siguientes:

200. En cuanto al tamaño de las claves, dependiendo de cada caso, es:

- AC FNMT raíz: RSA 4.096 bits.
- AC Subordinadas: RSA 2.048 bits.
- *Certificados de autenticación de sitios web:* RSA 2.048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

201. Las *Claves públicas* de los *Certificados de autenticación de sitios web* están codificadas de acuerdo con RFC5280 y PKCS#1.

6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3)

202. Los *Certificados* FNMT incluyen la extensión Key Usage y, según el caso, Extended Key Usage, indicando los usos habilitados de la *Claves*.

203. El *Certificado* raíz de la AC tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las AC Subordinadas y las ARLs. Los *Certificados* de las AC Subordinadas que expiden los *Certificados de autenticación de sitios web* tienen habilitado exclusivamente el uso para firmar/sellar *Certificados* de usuario final (*Certificados de autenticación de sitios web*) y CRLs.

204. El *Certificado de autenticación de sitios web* tiene habilitado el uso de firma digital (digital Signature). Adicionalmente, estos *Certificados* cuentan con el uso extendido de clave de autenticación de servidor (server authentication) y autenticación de cliente (client authentication).

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE LOS MÓDULOS CRIPTOGRÁFICOS

205. Véase el apartado correspondiente en la DGPC.

6.2.1. Estándares para los módulos criptográficos

206. Véase el apartado correspondiente en la DGPC.

6.2.2. Control multi-persona (n de m) de la clave privada

207. Véase el apartado correspondiente en la DGPC.

6.2.3. Custodia de la clave privada

208. Véase el apartado correspondiente en la DGPC.

6.2.4. Copia de seguridad de la clave privada

209. Véase el apartado correspondiente en la DGPC.

6.2.5. Archivado de la clave privada

210. Véase el apartado correspondiente en la DGPC.

6.2.6. Transferencia de la clave privada a/o desde el módulo criptográfico

211. Véase el apartado correspondiente en la DGPC.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

212. Véase el apartado correspondiente en la DGPC.

6.2.8. Método de activación de la clave privada

213. Véase el apartado correspondiente en la DGPC.

6.2.9. Método de desactivación de la clave privada

214. Véase el apartado correspondiente en la DGPC.

6.2.10. Método de destrucción de la clave privada

215. Véase el apartado correspondiente en la DGPC.

6.2.11. Clasificación de los módulos criptográficos

216. Véase el apartado correspondiente en la DGPC.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. Archivo de la clave pública

217. Los *Certificados de autenticación de sitios web* y, por tanto, sus *Claves públicas* asociadas, son conservadas por la FNMT-RCM durante el periodo de tiempo exigido por la legislación vigente, que actualmente es de 15 años.

6.3.2. Periodos operativos del certificado y periodos de uso del par de claves

218. Los periodos de operación de los Certificados y sus Claves asociadas son:

- *Certificado* de la AC FNMT raíz y su par de *Claves*: hasta el 1 de enero de 2030.

- El *Certificado* de la AC subordinada que expide los *Certificados de Firma Electrónica y Sello Electrónico* y su par de *Claves*: hasta el 21 de mayo de 2022.
- Los *Certificados de Sede* y su par de *Claves:* no superior a 12 meses.

6.4. DATOS DE ACTIVACIÓN

219. Véase el apartado correspondiente en la DGPC.

6.4.1. Generación e instalación de datos de activación

220. Véase el apartado correspondiente en la DGPC.

6.4.2. Protección de datos de activación

221. Véase el apartado correspondiente en la DGPC.

6.4.3. Otros aspectos de los datos de activación

222. Véase el apartado correspondiente en la DGPC.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

223. Véase el apartado correspondiente en la *DGPC*.

6.5.1. Requisitos técnicos específicos de seguridad informática

224. Véase el apartado correspondiente en la DGPC.

6.5.2. Evaluación del nivel de seguridad informática

225. Véase el apartado correspondiente en la DGPC.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

226. Véase el apartado correspondiente en la *DGPC*.

6.6.1. Controles de desarrollo de sistemas

227. Véase el apartado correspondiente en la DGPC.

6.6.2. Controles de gestión de la seguridad

228. Véase el apartado correspondiente en la DGPC.

6.6.3. Controles de seguridad del ciclo de vida

229. Véase el apartado correspondiente en la DGPC.

6.7. CONTROLES DE SEGURIDAD DE RED

230. Véase el apartado correspondiente en la *DGPC*.

6.8. FUENTE DE TIEMPO

231. Véase el apartado correspondiente en la *DGPC*.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

232. Los *Certificados de autenticación de sitios web* son de conformidad con el estándar europeo ETSI EN 319 412-4 "Certificate profile for web site certificates".

233. El *Certificado de Sede electrónica* contiene el identificador de política EV 0.4.0.2042.1.4.

7.1.1. Número de versión

234. Los *Certificados de autenticación de sitios web* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

235. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados de autenticación de sitios web*, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

236. El identificador de objeto (OID) correspondiente al algoritmo criptográfico utilizado (Sha256withRsaEncryption) es 1.2.840.113549.1.1.11.

7.1.4. Formatos de nombres

237. La codificación de los *Certificados de autenticación de sitios web* sigue la recomendación RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Todos los campos definidos en el perfil de estos *Certificados,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

7.1.5. Restricciones de nombres

238. Las CAs subordinadas que emiten los certificados bajo la presente DPPP no están restringidas técnicamente .

7.1.6. Identificador de objeto de política de certificado

239. El identificador de objeto (OID) de la política del *Certificados de autenticación de sitios web* es la definida en el apartado "1.2 Nombre del documento e identificación" del presente documento.

7.1.7. Empleo de la extensión restricciones de política

240. La extensión "Policy Constrains" del *Certificado* raíz de la AC no es utilizado.

7.1.8. Sintaxis y semántica de los calificadores de política

241. La extensión "Certificate Policies" incluye dos campos de "Policy Qualifiers":

- CPS Pointer: contiene la URL donde se publican las *Políticas de Certificación* y *Prácticas de Servicios de confianza* aplicables a este servicio.
- User notice: contiene el texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

7.1.9. Tratamiento semántico para la extensión "Certificate policy"

242. 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.

7.2. PERFIL DE LA CRL

7.2.1. Número de versión

243. El perfil de las CRL son conformes con el estándar X.509 versión 2.

7.2.2. CRL y extensiones

244. El perfil de las CRL sigue la siguiente estructura:

Tabla 3 – Perfil de la CRL

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption
Número de CRL	Valor incremental
Emisor	DN del emisor

Campos y extensiones	Valor
Fecha de emisión	Tiempo UTC de emisión.
Fecha de próxima actualización	Fecha de emisión + 24 horas
Identificador de la clave de Autoridad	Hash de la clave del emisor
ExpiredCertsOnCRL	NotBefore de la CA
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

245. El perfil de los mensajes OCSP emitidos por la FNMT-RCM, cumple con las especificaciones contenidas en el IETF RFC 6960 Internet X.509 PKI Online Certificate Status Protocol (OCSP) profile.

7.3.1. Número de versión

246. Los *Certificados* utilizados por el *Servicio de información y consulta sobre el estado de validez de los certificados*, vía OCSP, son conformes con el estándar X.509 versión 3.

7.3.2. Extensiones del OCSP

247. Véase el apartado correspondiente en la *DGPC*.

8. AUDITORÍAS DE CUMPLIMIENTO

248. El sistema de expedición de *Certificados de autenticación de sitios web* es sometido anualmente a un proceso de auditoría conforme a los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers" y ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

249. Adicionalmente, estos *Certificados* cuentan con la consideración de cualificados, por lo que la auditoría garantiza adicionalmente el cumplimiento de los requisitos de los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-4 "Certificate profile for web site certificates".

8.1. FRECUENCIA DE LAS AUDITORÍAS

250. Las auditorías mencionadas en el apartado anterior se realizan anualmente.

8.2. CUALIFICACIÓN DEL AUDITOR

251. Véase el apartado correspondiente en la *DGPC*.

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

252. Véase el apartado correspondiente en la *DGPC*.

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

253. Véase el apartado correspondiente en la *DGPC*.

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

254. Véase el apartado correspondiente en la *DGPC*.

8.6. COMUNICACIÓN DE LOS RESULTADOS

255. Véase el apartado correspondiente en la *DGPC*.

8.7. AUTOEVALUACIÓN

256. Véase el apartado correspondiente en la *DGPC*.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

257. Véase el apartado correspondiente en la *DGPC*.

9.1.1. Tarifas de emisión o renovación de certificados

258. La determinación de tarifas aplicables a la emisión o renovación de *Certificados* seguirá lo establecido en el apartado “9.1 Tarifas” del presente documento.

9.1.2. Tarifas de acceso a los certificados

259. No estipulado.

9.1.3. Tarifas de acceso a la información de estado o revocación

260. La FNMT-RCM ofrece los servicios de información del estado de los certificados a través de del protocolo OCSP de forma gratuita.

9.1.4. Tarifas para otros servicios

261. La determinación de tarifas aplicables a otros servicios seguirá lo establecido en el apartado "9.1 Tarifas" del presente documento.

9.1.5. Política de reembolso

262. La FNMT – RCM cuenta con una política de devolución que permite la solicitud de reembolso dentro del período de desistimiento establecido, aceptando que este hecho llevará consigo la revocación automática del certificado. El procedimiento se publica en la sede electrónica de la FNMT – RCM.

9.2. RESPONSABILIDAD FINANCIERA

263. Véase el apartado correspondiente en la *DGPC*.

9.2.1. Seguro de responsabilidad civil

264. Véase el apartado correspondiente en la DGPC.

9.2.2. Otros activos

265. Véase el apartado correspondiente en la DGPC.

9.2.3. Seguros y garantias para entidades finales

266. Véase el apartado correspondiente en la DGPC.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

267. Véase el apartado correspondiente en la *DGPC*.

9.3.1. Alcance de la información confidencial

268. Véase el apartado correspondiente en la DGPC.

9.3.2. Información no incluida en el alcance

269. Véase el apartado correspondiente en la DGPC.

9.3.3. Responsabilidad para proteger la información confidencial

270. Véase el apartado correspondiente en la DGPC.

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

271. Véase el apartado correspondiente en la *DGPC*.

9.4.1. Plan de privacidad

272. Véase el apartado correspondiente en la DGPC.

9.4.2. Información tratada como privada

273. Véase el apartado correspondiente en la DGPC.

9.4.3. Información no considerada privada

274. Véase el apartado correspondiente en la DGPC.

9.4.4. Responsabilidad de proteger la información privada

275. Véase el apartado correspondiente en la DGPC.

9.4.5. Aviso y consentimiento para usar información privada

276. Véase el apartado correspondiente en la DGPC.

9.4.6. Divulgación conforme al proceso judicial o administrativo

277. Véase el apartado correspondiente en la DGPC.

9.4.7. Otras circunstancias de divulgación de información

278. Véase el apartado correspondiente en la DGPC.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

279. Véase el apartado correspondiente en la *DGPC*.

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

280. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Suscriptor* del *Certificado* y, en su caso, con las partes usuarias y terceros que confían, quedarán determinadas, principalmente, por el documento relativo a las condiciones de utilización o el contrato de expedición del *Certificado*, y, subsidiariamente, por la presente *Declaración de Prácticas y Políticas de Certificación*.

281. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411 para la emisión de *Certificados* y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

282. La FNMT-RCM emite los *Certificados de sede electrónica* 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 dirección

https://cabforum.org/ Asimismo, adaptará sus prácticas de expedición de dichos *Certificados* a la versión vigente de los citados requisitos. En caso de cualquier incoherencia entre la presente *DPPP* y la citada versión, dichos requisitos prevalecerán sobre este documento.

283. Adicionalmente, la FNMT-RCM se compromete a cumplir, en relación con la expedición de los *Certificados de sede electrónica* emitidos bajo la presente política, los requisitos establecidos por la entidad CA/Browser fórum para este tipo de Certificados (EV SSL Certificate Guidelines), y que pueden consultarse en la dirección https://cabforum.org/extended-validation/. En caso de cualquier incoherencia entre la presente DPPP y la citada versión, dichos requisitos prevalecerán sobre este documento.

284. Sin perjuicio de lo dispuesto en la normativa de aplicación a este tipo de *Certificados*, así como las obligaciones descritas en el apartado correspondiente de la *DGPC*, el *Prestador de Servicios de Confianza* se obliga a:

285. 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.

  La identificación se realizará a través de *Certificados* cualificados de firma electrónica admitidos en los procesos de FNMT-RCM.

- 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* asociada a la *Clave Pública* que se incorpora al *Certificado* a emitir.

- Garantizar que los procedimientos seguidos aseguran que las *Claves Privadas* correspondientes a los *Certificados de autenticación de sitios web* son generadas 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.

9.6.2. Obligaciones de la AR

286. Véase el apartado correspondiente en la *DGPC*.

287. Las actividades relativas a la AR serán realizadas exclusivamente por la FNMT-RCM, a través de su Área de Registro, para todos los *Certificados de autenticación de sitios web.*

288. La AR, a través del Área de Registro de la FNMT-RCM, tiene las siguientes 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 relevantes para la finalidad asignada, de los *Solicitantes* de los *Certificados*, *Suscriptores* y sus *Representantes*, 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 *DPPP.*
- 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 autenticación de sitios web*, 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 dominio del *Certificado de autenticación de sitios web*, 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*.

9.6.3. Obligaciones de los Suscriptores

289. Véase el apartado correspondiente en la *DGPC*.

290. En cuanto a los *Certificados de autenticación de sitios web*, los *Suscriptores* han de tener el control del nombre de dominio de sitio web incluido en dichos *Certificados* y mantener bajo su uso exclusivo las *Claves privadas* asociadas.

291. El *Solicitante* y el *Suscriptor* de los *Certificados* expedidos bajo la presente *DPP*, 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, licenciatario o cuente 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 las *Claves privadas* asociadas,
- 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,* la *Firma electrónica* o el *Sello electrónico* avanzados 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.

292. 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.

293. 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.

294. 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.

295. En relación con los *Certificados de Sede electrónica*, las entidades públicas *Suscriptoras*, representadas a través de los diferentes órganos competentes, actuando a través del *Responsable de Operaciones de Registro* para la emisión de este tipo de *Certificados*, tienen la obligación de:

- No realizar registros o tramitar solicitudes de *Certificados de Sede electrónica* por personal que preste sus servicios en una entidad diferente a la que representa como *Oficina de Registro*, salvo habilitación expresa de otra entidad.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Suscriptor* se corresponda con una entidad pública sobre la que no tenga potestades o no tenga competencias para actuar como *Oficina de Registro*.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Suscriptor* no se corresponda con la titularidad de la dirección electrónica a través de la que se accede a la *Sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Solicitante* se corresponda con una *persona física* que no preste sus servicios en la entidad *Suscriptora* del *Certificado* y/o no haya sido autorizado por la persona que actúa como representante de la Entidad Pública para la gestión y administración de la dirección electrónica a través de la que se accede a la *Sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- Comprobar fehacientemente los datos identificativos y competenciales del *Suscriptor* del *Certificado* (la Entidad titular de la *Sede electrónica* y de la dirección electrónica, dominio o URL, a través del cual se accede a tal *Sede*) y del *Solicitante* (la persona física con atribución suficiente para solicitar un *Certificado* de *Sede electrónica*) del *Certificado* y verificar su correspondencia con el titular y contactos establecidos en las bases de datos correspondientes, para la gestión y administración de la dirección electrónica a través de la que se accede a la *Sede electrónica* que identificará el *Certificado* objeto de la solicitud.
- Solicitar la revocación del *Certificado de Sede electrónica* emitido bajo esta política cuando alguno de los datos referidos al *Suscriptor* o a la dirección electrónica incluida en el *Certificado* sean incorrectos, inexactos o hayan variado respecto a lo consignado en el *Certificado,* o no se correspondan con el titular y contactos establecidos en las bases de datos correspondientes para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación.

296. Las relaciones de la FNMT-RCM y el Suscriptor quedarán determinadas principalmente, a los efectos del régimen de uso de los Certificados, a través del documento relativo a las condiciones de utilización o en su caso, contrato de emisión del Certificado y atendiendo a los acuerdos, convenios o documento de relación entre la FNMT-RCM y la Entidad Pública correspondiente.

9.6.4. Obligaciones de las partes que confían

297. Véase el apartado correspondiente en la DGPC.

298. Será responsabilidad de la Entidad usuaria y de los terceros que confían en los Certificados la verificación y comprobación del estado de los Certificados, no cabiendo en ningún caso presumir la validez de los Certificados sin dichas comprobaciones.

299. Si las circunstancias indican necesidad de garantías adicionales, la Entidad Usuaria deberá obtener garantías adicionales para que dicha confianza resulte razonable.

300. 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.

9.6.5. Obligaciones de otros participantes

301. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

302. No estipulado.

9.8. LÍMITES DE RESPONSABILIDAD

303. Véase el apartado correspondiente en la *DGPC*.

9.9. INDEMNIZACIONES

304. Véase el apartado correspondiente en la *DGPC*.

9.9.1. Indemnización de la CA

305. No estipulado.

9.9.2. Indemnización de los Suscriptores

306. No estipulado.

9.9.3. Indemnización de las partes que confían

307. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

308. La presente *Declaración de Practicas y Políticas de Certificación* entrará en vigor en el momento de su publicación.

9.10.2. Terminación

309. La presente *Declaración de Practicas y Políticas de Certificación* será derogada en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente al documento anterior. La FNMT – RCM se compromete a someter dicha Declaración a un proceso de revisión anual.

9.10.3. Efectos de la finalización

310. Para los certificados vigentes emitidos bajo una *Declaración de Practicas y Políticas de Certificación* anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

311. Véase el apartado correspondiente en la *DGPC*.

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

312. Las modificaciones de la presente *Declaración de Prácticas y Políticas de Certificación* serán aprobadas por la Dirección del departamento Ceres, que quedarán reflejadas en la correspondiente acta del Comité de Gestión del Prestador, de conformidad con el procedimiento interno aprobado mediante el documento "Procedimiento de revisión y mantenimiento de las políticas de certificación y declaración de prácticas de servicios de confianza".

9.12.2. Periodo y mecanismo de notificación

313. Cualquier modificación en la presente *Declaración de Prácticas y Políticas de Certificación* será publicada de forma inmediata en la URL de acceso a las mismas.

314. Si las modificaciones a realizar no conllevan cambios significativos en cuanto al régimen de obligaciones y responsabilidades de las partes o relativos a una modificación de las políticas de prestación de los servicios, la FNMT-RCM no informará previamente a los usuarios, limitándose a publicar una nueva versión de la declaración afectada en su página web.

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

315. Las modificaciones significativas de las condiciones de los servicios, régimen de obligaciones y responsabilidades o limitaciones de uso pueden ocasionar un cambio de política del servicio y su identificación (OID), así como el enlace a la nueva declaración de política del servicio. En este caso, la FNMT-RCM podrá establecer un mecanismo de información de los cambios propuestos y, en su caso, de recogida de opiniones de las partes afectadas.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

316. Véase el apartado correspondiente en la *DGPC*.

9.14. NORMATIVA DE APLICACIÓN

317. Véase el apartado correspondiente en la *DGPC*.

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

318. La FNMT-RCM manifiesta su compromiso de cumplimiento de la normativa y de los requisitos de aplicación a cada tipo de *Certificado de autenticación de sitios web*, incluyendo las consideraciones establecidas en el apartado "1.5.4. Procedimiento de aprobación de la DPC" del presente documento de *DPPP*.

9.16. ESTIPULACIONES DIVERSAS

319. Véase el apartado correspondiente en la *DGPC*.

9.16.1. Acuerdo íntegro

320. Véase el apartado correspondiente en la DGPC.

9.16.2. Asignación

321. Véase el apartado correspondiente en la DGPC.

9.16.3. Severabilidad

322. Véase el apartado correspondiente en la DGPC.

9.16.4. Cumplimiento

323. Véase el apartado correspondiente en la DGPC.

9.16.5. Fuerza Mayor

324. Véase el apartado correspondiente en la DGPC.

9.17. OTRAS ESTIPULACIONES

325. Véase el apartado correspondiente en la *DGPC*.