POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE LOS CERTIFICADOS DE SELLO ELECTRÓNICO PARA SECTOR PÚBLICO

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	19/01/2026
Revisado por:	FNMT-RCM	19/01/2026
Aprobado por:	FNMT-RCM	19/01/2026

Versión	Fecha	Descripción
1.0	19/01/2026	Creación del documento

Referencia: DPC/ CPSELSP0100/SGPSC/2026

Documento clasificado como: *Público*

Índice de contenidos

Índice de tablas

1. INTRODUCCIÓN

1. El Artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social habilita la prestación de servicios de seguridad por parte de la Fábrica Nacional de Moneda y Timbre, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos, en su apartado Uno, establece que:

   "sin perjuicio de las competencias atribuidas en la Ley a los órganos administrativos en materia de registro de solicitudes, escritos y comunicaciones, se faculta a la Fábrica Nacional de Moneda y Timbre (FNMT) para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en las relaciones que se produzcan entre:

   a) *Los órganos de la Administración General del Estado entre sí o con los organismos públicos vinculados o dependientes de aquélla, así como las de estos organismos entre sí.*
   b) *Las personas físicas y jurídicas con la Administración General del Estado (AGE) y los organismos públicos vinculados o dependientes de ella"*

2. De otro lado, su apartado Dos, establece:

   "Asimismo, se habilita a la FNMT a prestar, en su caso, a las Comunidades Autónomas, las entidades locales y las entidades de Derecho público vinculadas o dependientes de ellas, los servicios a que se refiere el apartado anterior, en las relaciones que se produzcan a través de técnicas y medios EIT entre sí, con la Administración General del Estado o con personas físicas y jurídicas; siempre que, previamente, se hayan formalizado los convenios o acuerdos procedentes."

3. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, consagró el derecho de los ciudadanos a relacionarse electrónicamente con las diferentes Administraciones Públicas. El marco jurídico resultante de la aprobación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, viene a sistematizar toda la regulación relativa al procedimiento administrativo, clarificando e integrando el contenido de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y de la citada Ley 11/2007, de 22 de junio. Así mismo, 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, regula los sistemas de identificación y firma electrónicas utilizados en el ámbito de la Administración de Justicia.

4. La FNMT-RCM viene expidiendo este tipo de *Certificados*, como medio de identificación y de firma electrónica, desde los primeros años de aplicación de la citada Ley 11/2007.

5. En un entorno en el que la utilización de los medios electrónicos ha de ser lo habitual, la firma, el intercambio electrónico de datos en entornos cerrados de comunicación y la *Actuación administrativa automatizada*, con la obligación de que las Administraciones Públicas se

relacionen entre sí por medios electrónicos, requieren de los correspondientes sistemas de identificación, firma y sellos electrónicos.

6. Entre los mencionados sistemas de identificación, firma y sellos electrónicos admitidos en el actual marco jurídico se encuentran los *Certificados electrónicos* a los que se refiere la presente Declaración.

7. 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 (Reglamento eIDAS), establece un marco jurídico general para el uso de las *Firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos , los servicios de entrega electrónica certificada y los servicios de Certificados para la autenticación de sitios web.*

1.1. OBJETO

8. El presente documento tiene por objeto la información pública de las condiciones y características de los servicios de confianza y, especialmente, los servicios de emisión de *Certificados* electrónicos por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo, en particular las obligaciones y procedimientos que se compromete a cumplir en relación con la emisión de *Certificados de Sello Electrónico*, así como las obligaciones que se compromete a cumplir en relación con:

   - la gestión de los *Datos de creación y verificación de Firma* y de los *Certificados*, las condiciones aplicables a la solicitud, emisión, uso y extinción de la vigencia de los *Certificados* y sus *Datos de creación de Firma*, y en su caso, la existencia de procedimientos de coordinación con los Registros Públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros
   - la prestación del servicio de consulta del estado de validez de los *Certificados.*

9. 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.

10. Los *Certificados* emitidos por la FNMT-RCM bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* son *Certificados Cualificados,* conforme al citado

Reglamento eIDAS, así como a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y a 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.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

11. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Confianza* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* (*DGPC*) de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de confianza de la Entidad y, de otro lado, por los apartados específicos del presente documento de *Políticas de Certificación y Prácticas de Certificación Particulares*. No obstante lo anterior, la *Ley de Emisión* de cada tipo de *Certificado* o grupo de *Certificados* podrá establecer características especiales aplicables a los órganos, organismos, entidades y personal usuarios de los servicios de confianza de la FNMT-RCM.

12. De acuerdo con lo anterior, la estructura de la *Declaración de Prácticas de Certificación de la FNMT-RCM* es la siguiente:

a. Por una parte, la ***Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica***, que debe considerarse cuerpo principal de la *Declaración de Prácticas de Certificación* en el que se describe el régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica*, los controles de seguridad aplicados a los procedimientos e instalaciones de la FNMT-RCM, en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, 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 general que deben ponerse a disposición del público, independientemente de su papel en la Comunidad Electrónica.

b. Y, por otra parte, para cada servicio de confianza o conjunto o grupo de *Certificados*, identificado y diferenciado del resto por su tipología y régimen particular o diferenciador, existe una ***Política de Certificación*** específica en la que se describen las obligaciones de las partes, los límites de uso de los *Certificados* y responsabilidades y unas ***Prácticas de Certificación Particulares*** que desarrollan los términos definidos en la política correspondiente y otorgan prestaciones adicionales o específicas sobre las generales establecidas en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

   Estas *Políticas de Certificación* y *Prácticas de Certificación Particulares* concretan lo articulado en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y, por tanto, son parte integrante de ella, conformando, ambos, la *Declaración de Prácticas de Certificación* de la FNMT-RCM. No obstante, sólo son de aplicación para el conjunto de *Certificados* caracterizado e identificado en las correspondientes *Políticas y Prácticas Particulares de Certificación* y pueden revestir, además, especialidades plasmadas a través de la *Ley de Emisión* del

Certificado o grupo de *Certificados* correspondiente, en caso de que existan características o funcionalidades específicas.

c. El presente documento representa, por tanto, las *Políticas de Certificación y Prácticas de Certificación Particulares* para los *Certificados de Sello Electrónico en el ámbito de la Administración.*

13. El presente documento se denomina *"Políticas y Prácticas de Certificación de certificados de Sello electrónico del Sector Público*", 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*".

14. 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 (DGPC)*.

15. 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.

16. En el presente documento se incluyen las siguientes *Políticas de Certificación* identificadas de la siguiente forma:

Nombre: Política de Certificación de *Certificado de Sello Electrónico para la Administración*

Referencia / OID[1] 1.3.6.1.4.1.5734.3.17.1

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Nombre: Política de Certificación de *Certificado de Sello Electrónico para la Administración G2*

Referencia / OID: 1.3.6.1.4.1.5734.3.22.2.0

Tipo de política asociada: QCP-l. OID: 0.4.0.194112.1.1

Versión: 1.0

Fecha de aprobación: 19/01/2026

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

[1] *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.

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

17. Los *Certificados de Sello electrónico* expedidos por la FNMT-RCM bajo esta política de certificación cuentan con las garantías necesarias para ser utilizados como sistema de identificación y sello para la *Actuación administrativa / judicial automatizada* de aquellas Administraciones, organismos o entidades de derecho público (y, en su caso, sus respectivas unidades organizativas) a las que se expiden dichos *Certificados*

18. La FNMT-RCM interpretará, registrará, mantendrá, y publicará los procedimientos referidos en este apartado, pudiendo además recibir comunicaciones de los interesados sobre estos asuntos a través de la información de contacto expresada en el apartado 1.5.2 Datos de contacto del presente documento.

1.3. PARTES INTERVINIENTES

19. 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* de los *Certificados*
4. Partes que confían
5. Otros participantes

1.3.1. Autoridad de Certificación

20. 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 Jerarquía RSA. dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas con algoritmia RSA. El *Certificado* raíz de esta AC viene identificado por la siguiente información:

Tabla 1 – Certificado de la AC FNMT raíz

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

Certificado de la AC FNMT raíz	
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) Autoridad de Certificación subordinada a la raíz de RSA: expide los Certificados de entidad final objeto de la presente *DPPP*. El *Certificado* de dicha Autoridad viene identificado por la siguiente información:

Tabla 2 – Certificado de la AC SECTOR PÚBLICO subordinada

Certificado de la AC subordinada	
Sujeto	CN=AC Sector Público, ORG_ID=VATES-Q2826004J, OU=Ceres, O=FNMT-RCM,C=ES
Emisor	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES
Número de serie (hex)	34 81 60 C5 1F 5E DB CB 5D DF 89 CA B4 57 33 92
Validez	No antes: 28 de noviembre de 2019 No después: 28 de noviembre de 2029
Longitud clave pública	RSA 4096 bits
Algoritmo de firma	RSA – SHA256

Certificado de la AC subordinada	
Identificador de clave	E7 04 EE 70 91 11 92 44 F9 0E 92 8F 56 43 1E 07 1D BF 04 9C

c) Autoridad de Certificación raíz Jerarquía de Curvas Elípticas. dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas con algoritmia de curva elíptica. El *Certificado* raíz de esta AC viene identificado por la siguiente información:

Tabla 3 – Certificado de la AC FNMT raíz G2

Certificado de la AC RAÍZ FNMT-RCM G2	
Sujeto	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Emisor	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM, C=ES
Número de serie (hex)	1F B6 4F 91 9E C5 01 EA B1 21 28 BB 11 7A 00 3C 7C 5A EF 1A
Validez	No antes: 10 de Octubre de 2024. No después: 4 de Octubre de 2049
Longitud clave pública	EC 384 bits (P-384)
Algoritmo de firma	ecdsa-with-SHA384
Identificador de clave	E2 29 99 47 2A FF 5B 26 8A C8 34 41 66 45 AF 52 3A 08 F1 80

d) Autoridad de Certificación subordinada a la raíz de curva elíptica: expide los Certificados de entidad final objeto de la presente *DPPP*. El *Certificado* de dicha Autoridad viene identificado por la siguiente información:

Tabla 4 – Certificado de la AC ENTIDADES subordinada G2

Certificado de la AC subordinada G2	
Sujeto	CN=AC ENTIDADES G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM,C=ES
Emisor	CN=AC RAIZ FNMT-RCM G2,ORG_ID=VATES-Q2826004J,O=FNMT-RCM,C=ES
Número de serie (hex)	18 BF C8 71 81 3B C9 80 31 03 F1 5B 70 50 70 C0 56 20 4F 3D
Validez	No antes: 10 de octubre de 2024 No después: 07 de octubre de 2039
Longitud clave pública	EC 256 bits (P-256)
Algoritmo de firma	ecdsa-with-SHA384
Identificador de clave	E5 36 ED E0 98 12 92 DA 14 1B AE E1 97 50 98 FF 05 C9 5B 30

1.3.2. Autoridad de Registro

21. La Autoridad de Registro realiza las tareas de identificación del *Solicitante* de los *Certificados*, así como la comprobación de la documentación acreditativa de las circunstancias que constan en los mismos, la validación y la aprobación de las solicitudes de emisión, revocación y, en su caso, la renovación de dichos *Certificados*.

22. La validación y aprobación de las solicitudes de emisión de los Sellos Electrónicos sólo se podrá llevar a cabo desde la *Autoridad de Registro* de la propia FNMT-RCM.

1.3.3. Suscriptores de los certificados

23. Los *Suscriptores* de los *Certificados de Sello Electrónico* son la Administración, organismos y entidades públicas representadas a través de los diferentes órganos competentes.

1.3.4. Partes que confían

24. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del *Firmante* / *Suscriptor*, que reciben y / o usan *Certificados* expedidos por la FNMT-RCM y, como tales, les es de aplicación lo establecido por la presente *DPPP* cuando deciden confiar efectivamente en tales *Certificados*.

1.3.5. Otros participantes

25. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

26. Los *Certificados de Sello Electrónico*, a los que aplica esta *DPPP* 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" , ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons" y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons".

27. Los *Certificados de Sello Electrónico* emitidos bajo esta *Política de Certificación* son expedidos a organismos y que forman parte de la *Comunidad Electrónica,* tal y como se define en el apartado *Definiciones* de la *DGPC* de la FNMT-RCM, y con objeto de garantizar el origen y la integridad de los contenidos mediante la creación del *Sello electrónico*.

28. Los *Certificados de Sello Electrónico*, emitidos bajo esta *Política de Certificación* son válidos como sistemas de identificación y creación de *Sello electrónico* de Administración Pública, órgano, organismo o entidad de derecho público, de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y con 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, a los efectos de identificación y autenticación de la competencia en la *Actuación administrativa automatizada* y la *Actuación judicial automatizada*. La *Ley de Emisión* de estos *Certificados* podrá determinar, en defecto de normativa específica, las condiciones de uso y régimen de estos *Certificados* que permitirán la atribución a las Administraciones, organismos y entidades de los diferentes actos y resoluciones realizados por el personal a su servicio o por los creadores del *Sello Electrónico* ; todo ello, sin modificación legal o variación respecto de la actuación que vienen realizando estas Administraciones Públicas en los soportes tradicionales.

1.4.2. Restricciones en el uso de los certificados

29. Constituyen límites de uso de los *Certificados de Sello Electrónico* la creación de sellos electrónicos de Administración Pública, organismo o entidad de derecho público, de conformidad con la Ley 40/2015, y con la Ley 18/2011, de 5 de julio, para la identificación y autenticación del ejercicio de la competencia y en la *Actuación administrativa / judicial automatizada* de la unidad organizativa perteneciente a una Administración, organismo o entidad pública.

30. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados de Sello Electrónico* y la Clave privada que se realicen por el Personal al servicio *de la Administración* en nombre de ésta, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos, así como de las consecuencias y efectos que pudieran producirse en el marco de reclamaciones o, en su caso, de posibles responsabilidades patrimoniales llevadas a cabo por terceros.

31. En cuanto a las actividades del personal de las *Oficinas de Registro*, la FNMT – RCM quedará sujeta a las obligaciones y responsabilidades derivadas de la legislación en materia de firma electrónica, sin perjuicio de las especialidades contenidas en el artículo 11 del RD 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas.

32. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

33. Para poder usar los *Certificados de Sello electrónico* dentro de los límites señalados y de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica*, y adquirir la condición de *Entidad Usuaria*.

34. En cualquier caso, si un tercero desea confiar en la *Firma o Sello electrónicos* realizados con uno de estos *Certificados* sin acceder al *Servicio de información sobre el estado de los Certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas de Certificación 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*.

35. Además, incluso dentro del ámbito de la *Comunidad Electrónica*, no se podrá emplear este tipo de *Certificados* para:

- Firmar o sellar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Usos particulares o privados, salvo para relacionarse con las Administraciones cuando éstas lo admitan.
- Firmar o sellar 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 por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*

- Prestar servicios de notificación

- Cualquier uso que exceda de la finalidad de este tipo de *Certificados* sin la autorización previa de la FNMT-RCM.

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

36. 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 esta *Declaración de Prácticas y Políticas de Certificación*.

1.5.2. Datos de contacto

37. 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: +34 91 740 69 82

38. 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 (CPR) a la cuenta de correo electrónico: incidentes.ceres@fnmt.es.

1.5.3. Responsables de adecuación de la DPC

39. 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

40. La FNMT-RCM a través de su Comité de Gestión del *Prestador de Servicios de Confianza*, vela por el cumplimiento de la presente *Declaración de Políticas y Prácticas de Certificación*, las aprueba, revisa y actualiza al menos cada 365 días para mantenerlas 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

41. 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:

- *Actuación administrativa/judicial automatizada*: Actuación administrativa / judicial producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.
- *Certificado de Sello Electrónico*: Declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona. Se utiliza para la automatización de procesos de firma y autenticación entre componentes informáticos.
- *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.
- *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 Reglamento eIDAS.
- *Personal al servicio de la Administración*: Funcionarios, personal laboral, estatutario a su servicio, personal autorizado o personal al servicio de la Administración Pública o de la Administración de Justicia, órgano, organismo público o entidad de derecho público.
- *Responsable de Operaciones de Registro*: Persona física nombrada por el representante de la Administración pública, organismo público o entidad de derecho público, bajo cuya responsabilidad se realizan las tareas asignadas a la *Oficina de Registro*, con las obligaciones y responsabilidades asignadas en las presentes *Políticas y Prácticas de Certificación Particulares*.
- *Suscriptor*: La administración pública, órgano, organismo público o entidad de derecho público.

1.6.2. Acrónimos

42. 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: Common Name (Nombre común)

CRL: Lista de *Certificados* revocados

DN: Distinguished Name (Nombre distintivo)

DPC: Declaración de Prácticas de Certificación

DGPC: Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica

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.

ETSI: European Telecommunications Standards Institute

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

LCP: Política de *Certificado* ligera (Lightweight Certificate Policy)

NCP: Política de *Certificado* Normalizado

NCP+: Política de *Certificado* Normalizado Extendida

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

OID: Identificador de Objeto (Object IDentifier)

PIN: Personal Identification Number (Número de identificación personal)

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

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

43. La FNMT-RCM, como *Prestador de Servicios de Confianza*, mantiene un repositorio de información pública, disponible en horario 24x7, todos los días del año, en la dirección:

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

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

44. La información relativa a la expedición de *Certificados* electrónicos objeto de la presente *DPPP* está publicada en la siguiente dirección:

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

2.3. FRECUENCIA DE PUBLICACIÓN

45. 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. Tal como se indica en el apartado 1.5.4 "Procedimiento de aprobación de la DPC", la frecuencia de revisión de las DPC será de al menos 365 días.

46. En cuanto a la frecuencia de publicación de CRL, se define en el apartado "4.9.7 Características adicionales. Frecuencia de publicación".

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

47. 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. NOMBRES

48. 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

49. 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*.

50. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificados Sello Electrónico,* la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite.

3.1.2. Significado de los nombres

51. 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).

52. El campo Common Name de los *Certificados de Sello Electrónico* es la denominación de sistema o aplicación de proceso automático. Se deberá asegurar que dicho nombre tenga sentido y no dé lugar a ambigüedades.

3.1.3. Seudónimos

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

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

54. 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

55. El nombre distintivo (*DN*) asignado a los *Certificados* expedidos a un *Suscriptor*, bajo las presentes DPPP y dentro del dominio del *Prestador de Servicios de Confianza,* será único.

3.1.6. Reconocimiento y autenticación de marcas registradas

56. La FNMT–RCM no asume compromiso alguno sobre el uso de signos distintivos, registrados o no, en la emisión de los *Certificados* expedidos bajo la presente *Política de Certificación.* Solo se permite la solicitud de *Certificados* que incluyan signos distintivos cuyo derecho de uso sea propiedad del *Titular* o se encuentre debidamente autorizado. La FNMT–RCM no está obligada a verificar previamente la titularidad o registro de los signos distintivos antes de la emisión de los *Certificados,* aunque figuren en registros públicos.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. Métodos para probar la posesión de la clave privada

57. La FNMT-RCM no genera ni almacena el par de *Claves* asociado a los *Certificados de Sello Electrónico* expedidos bajo la presente *Política de Certificación*, poniendo todos los mecanismos necesarios durante el proceso de *Solicitud* del Sello para garantizar que el *Responsable de Operaciones de Registro* y/o el representante del *Suscriptor* se encuentran en posesión de la *Clave Privada* asociada a la *Clave Pública* que se certificará.

3.2.2. Autenticación de la identidad de la organización

58. Con carácter previo al establecimiento de cualquier relación institucional con los *Suscriptores*, la FNMT-RCM informa, a través de los medios y direcciones web citadas en estas *Prácticas de Certificación Particulares* y, subsidiariamente, en la *DGPC*, acerca de las condiciones del servicio, así como de las obligaciones, garantías y responsabilidades de las

partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Confianza*.

59. Las actividades de comprobación de la identidad del *Personal al servicio de la Administración*, *Solicitantes* de los *Certificados*, serán realizadas por el personal autorizado de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión. Garantizando la identidad de la Administración, *Suscriptora* del *Certificado*, que se corresponde, en cada caso, con el organismo o entidad donde el personal presta sus servicios.

60. Para los *Certificados de Sello Electrónico* la FNMT-RCM considerará con competencia al efecto, cualquier solicitud de *Certificado de Sello Electrónico* que venga realizada por el *Responsable de Operaciones de Registro* correspondiente, en su condición de representante del *Suscriptor*.

61. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

3.2.3. Autenticación de la identidad de la persona física solicitante

62. Se hace constar que la FNMT-RCM, en función de la relación de personal usuario dependiente remitida por la Administración, organismos o entidad pública, considerará, bajo responsabilidad de los correspondientes órganos, organismos y/o entidades, que actuarán a través de las *Oficinas de Registro*, que este personal se encuentra con su cargo vigente, que su número de Identificación Personal, empleo o autorización es auténtico y está en vigor y, por tanto, habilitados para obtener y usar los *Certificados de Sello Electrónico*. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del citado personal, así como que estos requisitos se mantienen durante toda la vida del *Certificado*, al no ostentar, la FNMT-RCM, relación jurídica funcionarial, administrativa o laboral con tal personal, más allá del documento de condiciones de utilización o, en su caso, contrato de emisión, cuyo efecto es estrictamente instrumental para el desempeño de las funciones propias del cargo.

63. Las actividades de comprobación anteriores serán realizadas por los responsables de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión, y que se corresponde, en cada caso, con el organismo o entidad donde el personal presta sus servicios. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

64. El *Solicitante* de los *Certificados de Sello Electrónico* se corresponde con el *Responsable de Operaciones de Registro* y/o el representante del *Suscriptor* o persona en quien delegue la unidad organizativa que requiere identificarse o realizar la *Actuación administrativa / judicial automatizada* con este tipo de *Certificados* y que presta sus servicios en una Administración Pública, organismo público o entidad de derecho público bajo la que se enmarca dicha unidad organizativa.

65. La AR de la FNMT-RCM comprueba que el *Representante del Suscriptor* coincide con la persona física que solicita un *Certificado*, mediante la firma electrónica del formulario de

solicitud utilizando un *Certificado* cualificado de firma electrónica, garantizando así la autenticidad de su identidad.

3.2.4. Información no verificada del Suscriptor

66. Toda la información incorporada al *Certificado de Sello Electrónico* es verificada por la *Autoridad de Registro*.

3.2.5. Validación de la autorización

67. La Autoridad de Registro de la FNMT-RCM verifica que el solicitante de un Sello tiene suficiente capacidad de representación mediante su nombramiento como *Responsable de Operaciones de Registro* y 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 de representante de administrador único o solidario de la persona jurídica *Suscriptora* o un *Certificado* cualificado de *Personal al servicio de la Administración Pública*, para cuya expedición ha sido acreditada la capacidad de representación.

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

69. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de regeneración de claves.

70. Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado correspondiente al proceso de renovación de *Certificados* de este documento.

3.3.1. Renovación rutinaria

71. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de renovación rutinaria.

3.3.2. Renovación después de una revocación

72. Bajo las presentes Políticas de Certificación, la FNMT-RCM no contempla ningún proceso de renovación después de una revocación.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

73. Previa a la revocación efectiva de los *Certificados de Sello Electrónico*, la Autoridad de Registro identificará de forma fehaciente a los solicitantes de la Revocación para vincularlos con los datos únicos del *Certificado de Selo Electrónico* a revocar.

74. Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado correspondiente al proceso de revocación de *Certificados* de este documento.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

75. Únicamente podrán solicitar Certificados de Sello Electrónico los *Representantes del Suscriptor*, *Personal al Servicio de la Administración* o personas debidamente autorizados a solicitar el Certificado en nombre del Suscriptor.

4.1.2. Proceso de registro y responsabilidades

76. El Solicitante, a través de la aplicación web de solicitud de *Certificados* desarrollada a tal efecto, deberá aceptar las condiciones de uso del *Certificado* e introducir sus datos identificativos, tales como el NIF, primer apellido, NIF del organismo al que pertenece, entre otros y su dirección de correo electrónico a la que se enviará un código de solicitud. El *Responsable de Operaciones de Registro*, representante del *Suscriptor*, será el encargado de firmar y enviar el contrato de expedición del *Certificado* a la FNMT-RCM.

77. La AR de la FNMT-RCM, tras recibir esta información, comprobará la validez de la información de la solicitud firmada, así como el tamaño de las claves generadas.

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

79. El apartado 9.6 "Obligaciones y garantias" 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

80. El *Solicitante* aportará los datos requeridos y acreditará su identidad personal. La identificación y validación de la documentación se realiza en todos los casos desde la Oficina de la FNMT-RCM. Una vez recibido el contrato enviado y firmado por el *Responsable de Operaciones de Registro*, la FNMT-RCM actuará diligentemente para:

a. Comprobar que el *Suscriptor* del *Certificado* existe y sus datos son correctos.

b. Comprobar que la persona que firma el contrato es el *Responsable de Operaciones de Registro*, y por lo tanto, tiene permisos por parte del *Suscriptor* para proceder a la petición del *Certificado de Sello Electrónico*.

4.2.2. Aprobación o rechazo de la solicitud del certificado

81. La Autoridad de Registro que actúa en el proceso de expedición de Certificados es siempre la propia FNMT-RCM y, por tanto, no delega la validación a ninguna otra Autoridad de Registro.

82. La Autoridad de Registro de la FNMT-RCM, una vez realizadas las comprobaciones relativas a la prueba de posesión de la clave privada por parte del Representante del Suscriptor, así como la autenticación de la identidad de la Organización y de la persona *Solicitante* del Certificado, según se describe en el apartado "3.2 Validación inicial de la identidad" de la presente DPPP, determinará la aprobación o el rechazo de la solicitud del mismo.

83. En caso de que la información sea incorrecta, la AR rechazará la solicitud y se pondrá en contacto con el solicitante para informarle del motivo. De lo contrario, se procederá a la emisión del certificado.

84. La FNMT-RCM recabará de los *Solicitantes* aquella información recibida de la *Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenando la información exigida por la legislación de firma electrónica durante el periodo de quince (15) años tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.

85. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

4.2.3. Tiempo en procesar la solicitud

86. La solicitud aprobada de los *Certificados de Sello Electrónico*, se empleará el tiempo mínimo necesario desde la recepción por parte de la Oficina de Registro de la FNMT – RCM de toda la documentación necesaria para realizar las comprobaciones requeridas de forma previa a la expedición del *Certificado*. La FNMT-RCM pondrá a disposición del Solicitante un mecanismo de descarga del *Certificado*.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

87. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, la información que describe su relación con la Administración Pública, así como el código de solicitud obtenido en la fase de solicitud, se procederá a la emisión del *Certificado de Sello Electrónico*.

88. La emisión de *Certificados de Sello Electrónico* supone la generación de documentos electrónicos que confirman los datos a incorporar en el *Certificado*, así como su

correspondencia con la *Clave Pública* asociada. La emisión de *Certificados* de la FNMT-RCM sólo puede realizarla ella misma, en calidad de *Prestador de Servicios de Confianza*, no existiendo ninguna otra entidad u organismo con capacidad de emisión de los mismos. La *Autoridad de Certificación* de la FNMT-RCM solo acepta solicitudes de generación de *Certificados* provenientes de fuentes autorizadas. Todos los datos contenidos en cada solicitud están protegidos contra alteraciones a través de mecanismos de *Firma Electrónica o Sello Electrónicos* realizados mediante el uso de *Certificados* emitidos a dichas fuentes autorizadas.

89. La FNMT-RCM en ningún caso, incluirá en un *Certificado* información distinta de la aquí mostrada, ni circunstancias, atributos o límites distintos a los previstos en los acuerdos, convenios y, en su caso, a los previstos en la *Ley de Emisión* correspondiente.

90. En cualquier caso, la FNMT-RCM actuará eficazmente para:

- Comprobar que el *Solicitante* del *Certificado* utilice la *Clave Privada* correspondiente a la *Clave Publica* vinculada al *Certificado.* Para ello, la FNMT-RCM comprobará la correspondencia entre la *Clave Privada* y la *Clave Pública*.
- Lograr que la información incluida en el *Certificado* se base en la información proporcionada por la *Oficina de Registro* correspondiente.
- No ignorar hechos notorios que puedan afectar a la fiabilidad del *Certificado.*
- Lograr que el *DN* (nombre distintivo) asignado a un *Sujeto*, en el ámbito de la presente DPPP, sea único.

91. Para la emisión del *Certificado* se seguirán los siguientes pasos:

1. Composición de la estructura de datos que conforman el *Certificado*.

   Con los datos recogidos durante el proceso de solicitud del *Certificado*, se procede a componer el nombre distintivo (*DN*) conforme al estándar *X.500*, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.

   El atributo *CN* contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado*

2. Composición de la identidad alternativa de los *Certificados de Sello Electrónico*

   La identidad alternativa de estos Certificados es distribuida en una serie de atributos, de forma que sea más sencilla la obtención de los datos del Suscriptor. Para ello se utiliza la extensión subjectAltName definida en X.509 versión 3, y contiene la siguiente información:

   • en el subcampo DirectoryName, el nombre, denominación del componente y el NIF de la Entidad representada.

3. Generación del *Certificado* conforme al perfil del *Certificado que corresponda*.

92. El formato de los *Certificados*, expedidos por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Cualificados*, puede consultarse en la página http://www.cert.fnmt.es/dpcs/

4.3.2. Notificación de la emisión

93. Una vez emitido el *Certificado de Sello Electrónico*, la FNMT-RCM informará al *Personal al servicio de la Administración Pública* sobre la disponibilidad de *Certificado* para su descarga.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

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

95. En este proceso guiado de descarga de un *Certificado de Sello de Electrónico*, se le pedirá al *Representante del Suscriptor* que introduzca el nombre del componente, así como el correspondiente código de solicitud obtenido en dicho proceso.

96. Si el *Certificado de Sello Electrónico* aún no hubiera sido generado por cualquier motivo, el proceso le informará de este hecho.

4.4.2. Publicación del certificado por la AC

97. Los *Certificados* generados son almacenados en un repositorio seguro de la FNMT-RCM, con acceso restringido.

4.4.3. Notificación de la emisión a otras entidades

98. No se realizan notificaciones de emisión a otras entidades.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada y uso del certificado

99. 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 responsables sobre el control de las claves del *Certificado*, al *Personal al servicio de la Administración*.

100. Los *Certificados de Sello Electrónico* emitidos bajo esta Política de Certificación son válidos como sistemas de identificación y creación de Sello electrónico de Administración Pública, órgano, organismo o entidad de derecho público, de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y con 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, a los efectos de identificación y autenticación de la competencia en la *Actuación administrativa automatizada* y la actuación judicial automatizada.

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

101. Los terceros que confían en los *Sellos electrónicos* realizados con las *Claves privadas* asociadas al *Certificado* se atendrán a las obligaciones y responsabilidades definidas en la presente *DPPP*.

4.6. RENOVACIÓN DEL CERTIFICADO

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

4.6.1. Circunstancias para la renovación del certificado

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

4.6.2. Quién puede solicitar la renovación del certificado

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

4.6.3. Procesamiento de solicitudes de renovación del certificado

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

4.6.4. Notificación de la renovación del certificado

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

4.6.5. Conducta que constituye la aceptación de la renovación del certificado

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

4.6.6. Publicación del certificado renovado

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

4.6.7. Notificación de la renovación del certificado a otras entidades

109. 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

110. Bajo las presentes Políticas de Certificación, la renovación con regeneración de claves de los *Certificados* se realiza siempre emitiendo nuevas claves, siguiendo el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.1. Circunstancias para la renovación con regeneración de claves

111. Las claves de los *Certificados* se renovarán bajo los siguientes supuestos:

- Por caducidad próxima de las actuales claves a petición del solicitante de la renovación.
- Por compromiso de las claves u otra circunstancia de las recogidas en el apartado "*4.9 Revocación y suspensión del certificado"* de la presente *DPPP.*

4.7.2. Quién puede solicitar la renovación con regeneración de claves

112. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

113. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.4. Notificación de la renovación con regeneración de claves

114. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves

115. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.6. Publicación del certificado renovado

116. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.7. Notificación de la renovación con regeneración de claves a otras entidades

117. Se seguirá el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.8. MODIFICACIÓN DEL CERTIFICADO

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

4.8.1. Circunstancias para la modificación del certificado

119. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

120. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

121. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

122. No se estipula la modificación.

4.8.5. Conducta que constituye la aceptación de la modificación del certificado

123. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

124. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

125. No se estipula la modificación.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

126. Los *Certificados* 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.

127. 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*.

128. 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/

4.9.1. Circunstancias para la revocación

4.9.1.1 Circunstancias para la revocación del certificado del suscriptor

129. La solicitud de revocación de los *Certificados* podrá efectuarse durante el período de validez que consta en el *Certificado.*

130. Serán causas admitidas para la revocación de un *Certificado* las expuestas a continuación:

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

- La utilización por un tercero de la Clave Privada asociada al *Certificado*
- La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* o de la clave privada asociada al *Certificado.*
- La no aceptación de las nuevas condiciones que puedan suponer la expedición de nuevas *Declaraciones de Prácticas y Políticas de Certificación*, durante el periodo de un mes tras su publicación.

b) Resolución judicial o administrativa que así lo ordene.

c) Extinción o disolución de la personalidad jurídica del *Suscriptor*

d) Fallecimiento o incapacidad sobrevenida, total o parcial, del *Firmante* o del representante del *Suscriptor.*

e) Inexactitudes en los datos aportados por el *Solicitante* 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*, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

f) Contravención de una obligación sustancial de esta *Declaración de Prácticas y Políticas de Certificación* por parte del *Firmante* o del *Solicitante* del *Certificado* o por parte de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*

g) Violación o puesta en peligro del secreto de los Datos de Creación de Firma o de la Clave Privada.

h) Resolución del contrato suscrito entre el *Firmante* o el Suscriptor y la FNMT-RCM.

i) Contravención de una obligación sustancial de esta *Declaración de Prácticas y Políticas de Certificación* por parte de una *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.

j) Cese en la actividad del Prestador de Servicios de Confianza salvo que la gestión de los Certificados electrónicos expedidos por aquél sea transferida a otro Prestador de Servicios de Confianza.

k) 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.

131. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a i) del presente apartado, debiendo ser notificadas a esta entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo.

132. 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 i) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.

133. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado* y 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.

134. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma y Sello* o claves privadas asociados, la finalización de la relación y régimen de uso de dicho *Certificado* y su *Clave privada* con la FNMT-RCM

4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada

135. Se atenderá a lo dispuesto en el "Plan de Actuación ante Compromiso de la Infraestructura de Clave Pública de FNMT-RCM"

4.9.2. Quién puede solicitar la revocación

136. La revocación de un *Certificado* solamente podrá ser solicitada por:

- la *Autoridad de Certificación* y la *Autoridad de Registro*
- el *Suscriptor* a través de su representante o persona autorizada, en la Oficina de Registro habilitada a tal efecto
- en su caso, el *Firmante,* a través del teléfono habilitado para tal fin (previa identificación del Solicitante) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7, o bien a través de dicha Oficina de Registro.

137. La FNMT-RCM podrá revocar de oficio los *Certificados* en los supuestos recogidos en la presente Declaración de Prácticas y Políticas de Certificación.

4.9.3. Procedimiento de solicitud de la revocación

138. La solicitud de revocación de los *Certificados de Sello Electrónico* podrá efectuarse durante el período de validez que consta en el *Certificado*.

139. El proceso de revocación puede realizarse de forma ininterrumpida 24x7, a través del Servicio de Revocación telefónica puesto a disposición de los usuarios para esta finalidad, asegurando la revocación del *Certificado* en un plazo inferior a 24h.

140. Durante la revocación telefónica, el solicitante de la revocación tendrá que confirmar los datos que se le soliciten, y aportar aquellos que sean imprescindibles para la validación de forma inequívoca de su capacidad para solicitar dicha revocación.

141. Adicionalmente, se puede solicitar la revocación de cualquier *Certificado* a través de la *Oficina de Registro*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica. El proceso de revocación en la oficina de registro es el siguiente:

a. Para *Certificados de Sello Electrónico,* el solicitante de la revocación remitirá a la *Oficina de Registro* el formulario creado a tal efecto, debidamente cumplimentado y firmado. Una vez la *Oficina de Registro* reciba la documentación, comprobará y validará la información, así como la capacidad del solicitante para pedir la revocación, procediendo a revocar el *Certificado* si todo es correcto.

142. La única *Oficina de Registro* que puede validar las revocaciones de los *Certificados de Sello Electrónico* es la Oficina de la FNMT-RCM.

143. Tan pronto la revocación sea efectiva, será notificado a través de la dirección de correo electrónico el *Representante del Suscriptor* que solicita la revocación de un *Certificado de Sello Electrónico*

144. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, 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 causa de revocación. Una vez que un *Certificado* ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

145. Para informar de posibles compromisos de Claves Privada, uso indebido de certificados u otros tipos de fraude, conducta inapropiada o cualquier otro asunto relacionado con los

certificados, se puede enviar un informe de incidencia sobre certificado (CPR) a la dirección de correo incidentes.ceres@fnmt.es indicada en el apartado 1.5.2.

4.9.4. Periodo de gracia de la solicitud de revocación

146. 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

147. La FNMT – RCM procede a la revocación inmediata del *Certificado* en el momento de verificar la identidad del *Solicitante* o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa. En cualquier caso, la revocación efectiva del *Certificado* se realizará en menos de 24 horas desde la recepción de la solicitud de revocación.

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

148. Las terceras partes que confían y aceptan el uso de los *Certificados* emitidos por la FNMT – RCM están obligadas a verificar, por medio de uno de los mecanismos disponibles (Listas de Revocación CRL y/o OCSP), el estado de los *Certificados*:

- 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
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

4.9.7. Frecuencia de generación de CRLs

149. Las *Listas de Revocación* (*CRL*) de los *Certificados de Firma Electrónica y Sello Electrónico* 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

150. 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

151. 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

152. La comprobación en línea del estado de revocación de los *Certificados de Sello Electrónico* 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

153. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

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

4.9.13. Circunstancias para la suspensión

155. No se contempla la suspensión de *Certificados*.

4.9.14. Quién puede solicitar la suspensión

156. No se contempla la suspensión de *Certificados*.

4.9.15. Procedimiento para la petición de la suspensión

157. No se contempla la suspensión de *Certificados*.

4.9.16. Límites sobre el periodo de suspensión

158. No se contempla la suspensión de *Certificados*.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

159. 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

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

4.10.3. Características opcionales

161. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

162. La suscripción finalizará en el momento de extinción de la vigencia del *Certificado*, ya sea por expiración del periodo de vigencia o por revocación del mismo. De no llevarse a cabo la renovación del *Certificado* se considerará extinguida la relación entre el *Firmante* y la FNMT-RCM.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

163. La FNMT-RCM no recuperará las *Claves privadas* asociadas a los *Certificados*.

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

164. No estipulado.

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

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

5.1. CONTROLES DE SEGURIDAD FÍSICA

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

5.1.1. Ubicación de las instalaciones

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

5.1.2. Acceso Físico

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

5.1.3. Electricidad y Aire Acondicionado

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

5.1.4. Exposición al agua

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

5.1.5. Prevención y Protección contra incendios

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

5.1.6. Almacenamiento de Soportes

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

5.1.7. Eliminación de Residuos

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

5.1.8. Copias de Seguridad fuera de las instalaciones

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

5.2. CONTROLES DE PROCEDIMIENTO

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

5.2.1. Roles de Confianza

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

5.2.2. Número de personas por tarea

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

5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Roles que requieren segregación de funciones

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

5.3. CONTROLES DE PERSONAL

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

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

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

5.3.2. Procedimientos de verificación de antecedentes

182. Véase el apartado correspondiente en la *DGPC*

5.3.3. Requisitos de formación

183. Véase el apartado correspondiente en la *DGPC*

5.3.4. Requisitos y frecuencia de actuación formativa

184. Véase el apartado correspondiente en la *DGPC*

5.3.5. Secuencia y frecuencia de rotación laboral

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

5.3.6. Sanciones por acciones no autorizadas

186. Véase el apartado correspondiente en la *DGPC*

5.3.7. Requisitos de contratación de personal

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

5.3.8. Suministro de documentación al personal

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

5.4. PROCEDIMIENTOS DE AUDITORÍA

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

5.4.1. Tipos de eventos registrados

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

5.4.2. Frecuencia de procesamiento de registros

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

5.4.3. Periodo de conservación de los registros

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

5.4.4. Protección de los registros

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

5.4.5. Procedimientos de copias de seguridad de los registros auditados

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

5.4.6. Sistemas de recolección de registros

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

5.4.7. Notificación al sujeto causante de los eventos

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

5.4.8. Análisis de vulnerabilidades

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

5.5. ARCHIVADO DE REGISTROS

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

5.5.1. Tipos de registros archivados

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

5.5.2. Periodo de retención del archivo

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

5.5.3. Protección del archivo

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

5.5.4. Procedimientos de copia de respaldo del archivo

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

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

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

5.5.6. Sistema de archivo

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

5.5.7. Procedimientos para obtener y verificar la información archivada

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

5.6. CAMBIO DE CLAVES DE LA AC

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

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

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

5.7.1. Gestión de incidentes y vulnerabilidades

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

5.7.2. Actuación ante datos y software corruptos

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

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

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

5.7.4. Continuidad de negocio después de un desastre

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

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

213. 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

214. En relación con la generación de las *Claves* de AC 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

215. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

216. En relación con la generación de las *Claves* del *Suscriptor*, la FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, que son generadas bajo el exclusivo control del *Responsable de Operaciones de Registro* o la persona autorizada por este.

6.1.2. Envío de la clave privada al suscriptor

217. No existe ninguna entrega de Clave privada en la emisión de los *Certificados* expedidos bajo las presentes *Políticas y Prácticas de Certificación*.

218. En todo caso, si la FNMT-RCM o cualquiera de las oficinas de registro tuviera conocimiento de un acceso no autorizado a la *Clave privada* del *Firmante*, el *Certificado* asociado a dicha *Clave privada* será revocado.

6.1.3. Envío de la clave pública al emisor del certificado

219. La *Clave pública,* generada junto a la *Clave privada* en un dispositivo de generación y custodia de claves, es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación.

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

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

6.1.5. Tamaños de claves y algoritmos utilizados

221. Los algoritmos utilizados bajo el ámbito de la presente *DPPP* son:

- RSA con SHA 256.

- ECDSA con SHA-384 y ECDSA con SHA-256

222. En cuanto al tamaño de las claves, son:

- de al menos 2048 bits en el caso de claves RSA
- de al menos 256 bits para el caso de claves ECDSA

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

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

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

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

225. El *Certificado* de las ACs FNMT raices tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

226. El *Certificado* de las AC FNMT Subordinadas que expide los *Certificados de Sello Electrónico* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.

227. Los *Certificados de Sello Electrónico* pueden tener habilitado exclusivamente los usos de encriptación, autenticación y firma.

228. La definición detallada de los perfiles de certificados finales y los usos admitidos de las claves se encuentra definidos en documento de perfiles de certificado disponible en http://www.cert.fnmt.es/dpcs/ .

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

6.2.1. Estándares para los módulos criptográficos

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

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

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

6.2.3. Custodia de la clave privada

231. Las operaciones de copia, salvaguarda o recuperación de las *Claves privadas* de las Autoridades de Certificación de la FNMT-RCM se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

6.2.4. Copia de seguridad de la clave privada

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

6.2.5. Archivado de la clave privada

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

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

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

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8. Método de activación de la clave privada

236. Las *Claves privadas* de las Autoridades de Certificación son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS PUB 140-2 Level 3.

237. Los mecanismos de activación y uso de las *Claves privadas* de la Autoridad de Certificación se basan en la segmentación de roles de gestión y operación que la FNMT-RCM tiene implementados con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes esquemas de uso simultáneo.

6.2.9. Método de desactivación de la clave privada

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

6.2.10. Método de destrucción de la clave privada

239. La FNMT-RCM destruirá o almacenará de forma apropiada las Claves del Prestador de Servicios de Confianza una vez finalizado el período de validez de las mismas, con la finalidad de evitar su uso inapropiado.

6.2.11. Clasificación de los módulos criptográficos

240. 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

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

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

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

- Para la Jerarquía RSA:
  - *Certificado* de la AC raíz FNMT-RCM y su par de *Claves*: hasta el 1 de enero de 2030.
  - El *Certificado* de la AC Sector Público subordinada que expide los *Certificados de Sello Electrónico*: hasta el 28 de noviembre de 2029.
  - Los *Certificados de Sello de Electrónico y su* par de *Claves:* hasta el 31 de diciembre de 2028.
- Para la Jerarquía Curvas Elípticas:
  - *Certificado* de la AC raíz FNMT-RCM G2 y su par de *Claves*: hasta el 4 de octubre de 2049.
  - El *Certificado* de la AC Entidades G2 subordinada que expide los *Certificados de Sello Electrónicos*: hasta 07 de octubre de 2039.
  - Los *Certificados de Sello Electrónico G2* y su par de claves: no superior a 3 años.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

243. Los datos de activación, tanto de las *Claves* de la AC FNMT raíz como de las *Claves* de la AC subordinada que expide los *Certificados de Sello Electrónico* se generan durante la ceremonia de *Claves* de creación de dichas *Autoridades de Certificación*.

6.4.2. Protección de datos de activación

244. Los datos de activación de las *Claves privadas* de la *Autoridad de Certificación* están protegidos, conforme al método descrito en el apartado "6.2.8 Método de activación de la *Clave privada*" del presente documento, con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes esquemas de uso simultáneo.

6.4.3. Otros aspectos de los datos de activación

245. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

6.5.1. Requisitos técnicos específicos de seguridad informática

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

6.5.2. Evaluación del nivel de seguridad informática

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

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.6.1. Controles de desarrollo de sistemas

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

6.6.2. Controles de gestión de la seguridad

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

6.6.3. Controles de seguridad del ciclo de vida

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

6.7. CONTROLES DE SEGURIDAD DE RED

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

6.8. FUENTE DE TIEMPO

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

6.9. OTROS CONTROLES ADICIONALES

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

6.9.1. Control de la capacidad de prestación de los servicios

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

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

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

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

258. Los *Certificados de Sello Electrónico* son expedidos como "cualificados" de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons".

7.1.1. Número de versión

259. Los *Certificados de Sello Electrónico* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

260. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados de Sello Electrónico* emitidos bajo esta política, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

261. Los identificadores de objeto (OID) correspondientes a los algoritmos criptográficos utilizados son:

- Jerarquía RSA
  - Algoritmo *SHA-256 with RSA Encryption* cuyo OID es 1.2.840.113549.1.1.11
- Jerarquía Curva Elíptica:
  - Algoritmo *SHA-384 with ECDSA Encryption* cuyo OID es 1.2.840.10045.4.3.3
  - Algoritmo *SHA-256 with ECDSA Encryption* cuyo OID es 1.2.840.10045.4.3.2

7.1.4. Formatos de nombres

262. La codificación de los *Certificados de Sello Electrónico* 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.

263. En la página http://www.cert.fnmt.es/dpcs/ se publica el documento que describe el perfil de los *Certificados* emitidos bajo esta política, incluyendo todas sus extensiones.

7.1.5. Restricciones de nombres

264. El nombre distintivo (*DN*) asignado al *Sujeto* del *Certificado*, en el ámbito de la presente *DPPP*, será único y con la composición definida en el perfil del *Certificado*.

7.1.6. Identificador de objeto de política de certificado

265. El identificador de objeto (OID) de la política del *Certificado de Sello Electrónico* 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

266. La extensión "Policy Constrains" no se usa en ningún *Certificado* raíz (ni en AC RAIZ FNMT-RCM, ni en AC RAIZ FNMT-RCM G2).

7.1.8. Sintaxis y semántica de los calificadores de política

267. 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 un 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"

268. 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

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

7.2.2. CRL y extensiones

270. Los perfiles de las CRLs siguen las siguientes estructuras:

Tabla 5 – Perfiles de las CRL

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption o SHA-256 with ECDSA

Campos y extensiones	Valor
Número de CRL	Valor incremental
Emisor	DN del emisor
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
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
ExpiredCertsOnCRL	NotBefore de la CA
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

7.3.1. Número de versión

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

7.3.2. Extensiones del OCSP

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

8. AUDITORÍAS DE CUMPLIMIENTO

273. El sistema de expedición de *Certificados* 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".

274. Así mismo, los Certificados tienen la consideración de cualificados, por lo que la auditoría garantiza el cumplimiento con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates".

275. El sistema de expedición de Certificados es sometido a otras auditorías adicionales:

- Auditoría del Sistema de Gestión de la Seguridad de la Información conforme a UNE-ISO/IEC 27001 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos".
- Auditoría del Sistema de Gestión de Privacidad de la Información conforme a UNE-ISO/IEC 27701 "Sistemas de Gestión de Privacidad de la Información (SGPI). Requisitos".
- Auditoría según lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 311/2022, del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).
- Auditoría del Sistema de Gestión de la Calidad con arreglo a ISO 9001.
- Auditoría del Sistema de Gestión de la Responsabilidad Social en correspondencia con IQNet SR10.
- Auditoría del Plan de continuidad de negocio según ISO 22301.
- Auditoría conforme el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (RGPD / LOPD-GDD).

276. También se llevan a cabo análisis de riesgos, de acuerdo con lo dictado en el Sistema de Gestión de la Seguridad de la Información.

8.1. FRECUENCIA DE LAS AUDITORÍAS

277. Periódicamente se elaborarán los correspondientes planes de auditorías.

278. La *Autoridad de Certificación* que expide los *Certificados de Sello Electrónico* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons". La auditoría es realizada anualmente por una empresa externa acreditada.

279. Un auditor independiente evaluará anualmente el cumplimiento por parte de la CA de los requisitos y prácticas establecidos en esta DPC.

280. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente.

8.2. CUALIFICACIÓN DEL AUDITOR

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

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

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

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

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

8.7. AUTOEVALUACIÓN

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

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

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

9.1.1. Tarifas de emisión o renovación de certificados

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

9.1.2. Tarifas de acceso a los certificados

289. No estipulado.

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

290. La FNMT-RCM ofrece los servicios de información del estado de los certificados a través de CRL o del OCSP de forma gratuita.

9.1.4. Tarifas para otros servicios

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

9.1.5. Política de reembolso

292. 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

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

9.2.1. Seguro de responsabilidad civil

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

9.2.2. Otros activos

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

9.2.3. Seguros y garantías para entidades finales

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

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.3.1. Alcance de la información confidencial

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

9.3.2. Información no incluida en el alcance

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

9.3.3. Responsabilidad para proteger la información confidencial

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

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

9.4.1. Plan de privacidad

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

9.4.2. Información tratada como privada

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

9.4.3. Información no considerada privada

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

9.4.4. Responsabilidad de proteger la información privada

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

9.4.5. Aviso y consentimiento para usar información privada

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

9.4.6. Divulgación conforme al proceso judicial o administrativo

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

9.4.7. Otras circunstancias de divulgación de información

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

310. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con el *Suscriptor* del *Certificado*, y con el resto de miembros de la *Comunidad Electrónica*, 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*.

311. La FNMT – RCM cumple los requisitos de las especificaciones técnicas de la norma ETSI EN 319 411-2 para la emisión de *Certificados* cualificados y se compromete a continuar cumpliendo con dicha norma o aquellas que la sustituyan.

312. El régimen de derechos y obligaciones de las Administraciones, organismos, entidades públicas y la FNMT-RCM se regirá mediante el correspondiente acuerdo o convenio regulador de la prestación de los servicios de confianza. En estos acuerdos o convenios podrá establecerse la *Ley de Emisión* de estos *Certificados* con el contenido y finalidad prevista en esta Declaración

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

9.6.2. Obligaciones de la AR

314. Las actividades relativas a la AR serán realizadas exclusivamente por la FNMT-RCM, a través de su Área de Registro.

315. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica, 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 *Solicitante* del *Certificado*, *Suscriptor* y/o su *Representante*, 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*. 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.
- 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*.

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

9.6.3. Obligaciones del suscriptor

317. El *Solicitante* responderá de que la información presentada durante la solicitud del *Certificado* es verdadera y que la solicitud y descarga del *Certificado* se realizan desde un equipo o dispositivo que puede utilizar, con un alto nivel de confianza, bajo su control exclusivo.

318. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Personal al servicio de la Administración Pública*, como *Solicitante* del *Certificado,* y/o en su caso el *Suscriptor* de los mismos, 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.
- Devolver o destruir el *Certificado* cuando así lo exija la FNMT-RCM, y no usarlo con propósito de firmar o identificarse electrónicamente cuando el *Certificado* caduque, o sea revocado.

319. 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.

320. 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.

321. 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.

322. 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

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

9.6.5. Obligaciones de otros participantes

324. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

325. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

326. De forma adicional a las responsabilidades enumeradas en la *DGPC,* el *Prestador de Servicios de Confianza*:

- No será responsable de la utilización de los *Certificados* emitidos bajo esta política cuando los representantes del *Suscriptor* del *Certificado* o *el Personal al Servicio de la Administración* realicen actuaciones sin facultades o extralimitándose de las mismas.
- En los *Certificados de Sello Electrónico* la FNMT-RCM no será responsable de la comprobación de la pertenencia de la unidad organizativa a consignar en el *Certificado* al órgano de la administración *Suscriptora* del *Certificado* ni de la pertenencia del *Solicitante* a la unidad organizativa como máximo responsable de ésta, correspondiendo esta actividad y responsabilidad de comprobación a la *Oficina de Registro*. FNMT-RCM considerará representante del órgano, organismo o entidad de la administración *Suscriptora* del *Certificado*, salvo que sea informada de lo contrario al *Responsable de Operaciones de Registro* correspondiente
- Las relaciones de la Administración Pública *Suscriptora* del *Certificado* y de su personal con la FNMT-RCM, se realizarán siempre a través de la *Oficina de Registro* y su responsable.

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

9.9. INDEMNIZACIONES

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

9.9.1. Indemnización de la CA

329. No estipulado.

9.9.2. Indemnización de los Suscriptores

330. No estipulado.

9.9.3. Indemnización de las partes que confían

331. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

333. La presente *Declaración de Prácticas 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

334. Para los *Certificados* vigentes emitidos bajo una *Declaración de Prácticas 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

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

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

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

9.12.2. Periodo y mecanismo de notificación

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

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

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

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA DE APLICACIÓN

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

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

341. La FNMT-RCM manifiesta el cumplimiento de la normativa de aplicación.

9.16. ESTIPULACIONES DIVERSAS

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

9.16.1. Acuerdo íntegro

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

9.16.2. Asignación

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

9.16.3. Severabilidad

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

9.16.4. Cumplimiento

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

9.16.5. Fuerza Mayor

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

9.17. OTRAS ESTIPULACIONES

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