Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN, FIRMA ELECTRÓNICA Y SELLO ELECTRÓNICO DEL SECTOR PÚBLICO

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	14/06/2024
Revisado por:	FNMT-RCM	21/06/2024
Aprobado por:	FNMT-RCM	24/06/2024

Versión	Fecha	Descripción
1.0	13/11/2019	Declaración de Prácticas y Políticas de Certificación de certificados de firma electrónica y sello electrónico del Sector Público
1.1	29/06/2020	Inclusión Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia
1.2	28/04/2021	Revisión general. Apdo. 4.9.12: referencia a DGPC
1.3	26/10/2021	Inclusión del Certificado de empleado público en QSCD
1.4	15/02/2023	Inclusión en el Apdo. 4.9.1.1 el caso de pérdida de la certificación como QSCD.
1.5	28/08/2023	Inclusión del Certificado de firma de empleado público en QSCD nivel alto y Certificado de autenticación de empleado público en QSCD nivel alto
1.6	23/05/2024	Actualización de Políticas de Certificación.
1.7	24/06/2024	Actualización validaciones de cuenta en el Portal de Gestión de Identidades.

Referencia: DPC/DPCSP_0107/SGPSC/2024

Documento clasificado como: *Público*

Índice de contenidos

1. Introducción 9

1.1. Objeto 10

1.2. Nombre del documento e identificación 11

1.3. Partes intervinientes 15
1.3.1. Autoridad de Certificación 15
1.3.2. Autoridad de Registro 17
1.3.3. Firmantes 17
1.3.4. Suscriptores de los certificados 17
1.3.5. Partes que confían 17
1.3.6. Otros participantes 17

1.4. Uso de los certificados 18
1.4.1. Usos permitidos de los certificados 18
1.4.2. Restricciones en el uso de los certificados 19

1.5. Administración de Políticas 21
1.5.1. Entidad responsable 21
1.5.2. Datos de contacto 21
1.5.3. Responsables de adecuación de la DPC 21
1.5.4. Procedimiento de aprobación de la DPC 21

1.6. Definiciones y Acrónimos 22
1.6.1. Definiciones 22
1.6.2. Acrónimos 24

2. Publicación y repositorios 25

2.1. Repositorio 25

2.2. Publicación de información de certificación 25

2.3. Frecuencia de publicación 25

2.4. Control de acceso a los repositorios 25

3. Identificación y autenticación 26

3.1. Nombres 26
3.1.1. Tipos de nombres 26
3.1.2. Significado de los nombres 26
3.1.3. Seudónimos 26
3.1.4. Reglas utilizadas para interpretar varios formatos de nombres 26
3.1.5. Unicidad de los nombres 27
3.1.6. Reconocimiento y autenticación de marcas registradas 27

3.2. Validación inicial de la identidad 27
3.2.1. Métodos para probar la posesión de la clave privada 27
3.2.2. Autenticación de la identidad de la organización 28
3.2.3. Autenticación de la identidad de la persona física solicitante 28
3.2.3.1. Comprobación directa mediante presencia física 29

3.2.3.2. Comprobación utilizando medios de identificación electrónica 29
3.2.3.3. Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional 30
3.2.4. Información no verificada del Suscriptor 30
3.2.5. Validación de la autorización 30
3.2.6. Criterios de interoperación 30

3.3. Identificación y autenticación para peticiones de renovación de claves 31
3.3.1. Renovación rutinaria 31
3.3.2. Renovación después de una revocación 31

3.4. Identificación y autenticación para peticiones de revocación 31

4. Requisitos operativos del ciclo de vida de los certificados 31

4.1. Solicitud de Certificados 31
4.1.1. Quién puede solicitar un Certificado 31
4.1.2. Proceso de registro y responsabilidades 31

4.2. Procedimiento de solicitud de certificados 32
4.2.1. Realización de las funciones de identificación y autenticación 32
4.2.2. Aprobación o rechazo de la solicitud del certificado 33
4.2.3. Tiempo en procesar la solicitud 33

4.3. Emisión del certificado 33
4.3.1. Acciones de la AC durante la emisión 33
4.3.2. Notificación de la emisión 35

4.4. Aceptación del certificado 35
4.4.1. Proceso de aceptación 35
4.4.2. Publicación del certificado por la AC 35
4.4.3. Notificación de la emisión a otras entidades 35

4.5. Par de claves y uso del certificado 36
4.5.1. Clave privada y uso del certificado 36
4.5.2. Uso del certificado y la clave pública por terceros que confían 36

4.6. Renovación del certificado 36
4.6.1. Circunstancias para la renovación del certificado 36
4.6.2. Quién puede solicitar la renovación del certificado 36
4.6.3. Procesamiento de solicitudes de renovación del certificado 37
4.6.4. Notificación de la renovación del certificado 37
4.6.5. Conducta que constituye la aceptación de la renovación del certificado 37
4.6.6. Publicación del certificado renovado 37
4.6.7. Notificación de la renovación del certificado a otras entidades 37

4.7. Renovación con regeneración de las claves del certificado 37
4.7.1. Circunstancias para la renovación con regeneración de claves 37
4.7.2. Quién puede solicitar la renovación con regeneración de claves 37
4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves 38
4.7.4. Notificación de la renovación con regeneración de claves 38
4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves 38
4.7.6. Publicación del certificado renovado 38
4.7.7. Notificación de la renovación con regeneración de claves a otras entidades 38

4.8. Modificación del certificado 38
4.8.1. Circunstancias para la modificación del certificado 38
4.8.2. Quién puede solicitar la modificación del certificado 38
4.8.3. Procesamiento de solicitudes de modificación del certificado 38
4.8.4. Notificación de la modificación del certificado 38
4.8.5. Conducta que constituye la aceptación de la modificación del certificado 38
4.8.6. Publicación del certificado modificado 39
4.8.7. Notificación de la modificación del certificado a otras entidades 39

4.9. Revocación y Suspensión del certificado 39
4.9.1. Circunstancias para la revocación 39
4.9.1.1 Circunstancias para la revocación del certificado del suscriptor 39
4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada 41
4.9.2. Quién puede solicitar la revocación 41
4.9.3. Procedimiento de solicitud de la revocación 41
4.9.4. Periodo de gracia de la solicitud de revocación 42
4.9.5. Plazo de tiempo para procesar la solicitud de revocación 43
4.9.6. Obligación de verificar las revocaciones por las partes que confían 43
4.9.7. Frecuencia de generación de CRLs 43
4.9.8. Periodo máximo de latencia de las CRLs 43
4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados 43
4.9.10. Requisitos de comprobación en línea de la revocación 43
4.9.11. Otras formas de aviso de revocación disponibles 44
4.9.12. Requisitos especiales de revocación de claves comprometidas 44
4.9.13. Circunstancias para la suspensión 44
4.9.14. Quién puede solicitar la suspensión 44
4.9.15. Procedimiento para la petición de la suspensión 44
4.9.16. Límites sobre el periodo de suspensión 44

4.10. Servicios de información del estado de los certificados 44
4.10.1. Características operativas 44
4.10.2. Disponibilidad del servicio 44
4.10.3. Características opcionales 44

4.11. Finalización de la suscripción 45

4.12. Custodia y recuperación de claves 45
4.12.1. Prácticas y políticas de custodia y recuperación de claves 45
4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión 45

5. Controles de seguridad física, de procedimientos y de personal 45

5.1. Controles de Seguridad Física 45
5.1.1. Ubicación de las instalaciones 45
5.1.2. Acceso Físico 45
5.1.3. Electricidad y Aire Acondicionado 46
5.1.4. Exposición al agua 46
5.1.5. Prevención y Protección contra incendios 46
5.1.6. Almacenamiento de Soportes 46
5.1.7. Eliminación de Residuos 46
5.1.8. Copias de Seguridad fuera de las instalaciones 46

5.2. Controles de Procedimiento 46

5.2.1. Roles de Confianza 46
5.2.2. Número de personas por tarea 46
5.2.3. Identificación y autenticación para cada rol 46
5.2.4. Roles que requieren segregación de funciones 46

5.3. Controles de Personal 47
5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos 47
5.3.2. Procedimientos de verificación de antecedentes 47
5.3.3. Requisitos de formación 47
5.3.4. Requisitos y frecuencia de actuación formativa 47
5.3.5. Secuencia y frecuencia de rotación laboral 47
5.3.6. Sanciones por acciones no autorizadas 47
5.3.7. Requisitos de contratación de personal 47
5.3.8. Suministro de documentación al personal 47

5.4. Procedimientos de auditoría 47
5.4.1. Tipos de eventos registrados 47
5.4.2. Frecuencia de procesamiento de registros 48
5.4.3. Periodo de conservación de los registros 48
5.4.4. Protección de los registros 48
5.4.5. Procedimientos de copias de seguridad de los registros auditados 48
5.4.6. Sistemas de recolección de registros 48
5.4.7. Notificación al sujeto causante de los eventos 48
5.4.8. Análisis de vulnerabilidades 48

5.5. Archivado de registros 48
5.5.1. Tipos de registros archivados 48
5.5.2. Periodo de retención del archivo 48
5.5.3. Protección del archivo 48
5.5.4. Procedimientos de copia de respaldo del archivo 49
5.5.5. Requisitos para el sellado de tiempo de los registros of Records 49
5.5.6. Sistema de archivo 49
5.5.7. Procedimientos para obtener y verificar la información archivada 49

5.6. Cambio de claves de la AC 49

5.7. Gestión de incidentes y vulnerabilidades 49
5.7.1. Gestión de incidentes y vulnerabilidades 49
5.7.2. Actuación ante datos y software corruptos 49
5.7.3. Procedimiento ante compromiso de la clave privada de la AC 49
5.7.4. Continuidad de negocio después de un desastre 49

5.8. Cese de la actividad del Prestador de Servicios de Confianza 50

6. Controles de seguridad técnica 50

6.1. Generación e instalación de las Claves 50
6.1.1. Generación del par de claves 50
6.1.1.1 Generación del par de Claves de la CA 50
6.1.1.2 Generación del par de Claves de la RA 50
6.1.1.3 Generación del par de Claves de los Suscriptores 50
6.1.2. Envío de la clave privada al suscriptor 51
6.1.3. Envío de la clave pública al emisor del certificado 51

6.1.4. Distribución de la clave pública de la AC a las partes que confían 51
6.1.5. Tamaños de claves y algoritmos utilizados 51
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad 51
6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3) 51

6.2. Protección de la clave privada y controles de los módulos criptográficos 52
6.2.1. Estándares para los módulos criptográficos 52
6.2.2. Control multi-persona (n de m) de la clave privada 52
6.2.3. Custodia de la clave privada 52
6.2.4. Copia de seguridad de la clave privada 52
6.2.5. Archivado de la clave privada 53
6.2.6. Trasferencia de la clave privada a o desde el módulo criptográfico 53
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico 53
6.2.8. Método de activación de la clave privada 53
6.2.9. Método de desactivación de la clave privada 53
6.2.10. Método de destrucción de la clave privada 53
6.2.11. Clasificación de los módulos criptográficos 53

6.3. Otros aspectos de la gestión del par de claves 54
6.3.1. Archivo de la clave pública 54
6.3.2. Periodos de operación del certificado y periodos de uso del par de claves 54

6.4. Datos de activación 54
6.4.1. Generación e instalación de datos de activación 54
6.4.2. Protección de datos de activación 54
6.4.3. Otros aspectos de los datos de activación 55

6.5. Controles de seguridad informática 55
6.5.1. Requisitos técnicos específicos de seguridad informática 55
6.5.2. Evaluación del nivel de seguridad informática 55

6.6. Controles técnicos del ciclo de vida 55
6.6.1. Controles de desarrollo de sistemas 55
6.6.2. Controles de gestión de la seguridad 55
6.6.3. Controles de seguridad del ciclo de vida 55

6.7. Controles de seguridad de red 55

6.8. Fuente de tiempo 55

6.9. Otros controles adicionales 56
6.9.1. Control de la capacidad de prestación de los servicios 56
6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas 56

7. Perfiles de los certificados, CRLs y OCSP 56

7.1. Perfil del certificado 56
7.1.1. Número de versión 56
7.1.2. Extensiones del certificado 56
7.1.3. Identificadores de objeto de algoritmos 56
7.1.4. Formatos de nombres 57
7.1.5. Restricciones de nombres 57
7.1.6. Identificador de objeto de política de certificado 57
7.1.7. Empleo de la extensión restricciones de política 57

7.1.8. Sintaxis y semántica de los calificadores de política 57
7.1.9. Tratamiento semántico para la extensión "certificate policy" 57

7.2. Perfil de la CRL 58
7.2.1. Número de versión 58
7.2.2. CRL y extensiones 58

7.3. Perfil de OCSP 59
7.3.1. Número de versión 59
7.3.2. Extensiones del OCSP 59

8. Auditorías de cumplimiento 59

8.1. Frecuencia de las Auditorías 59

8.2. Cualificación del auditor 60

8.3. Relación del auditor con la empresa auditada 60

8.4. Elementos objetos de auditoría 60

8.5. Toma de decisiones frente a detección de deficiencias 60

8.6. Comunicación de los resultados 60

8.7. autoevaluación 60

9. Otros asuntos legales y de actividad 61

9.1. Tarifas 61
9.1.1. Tarifas de emisión o renovación de certificados 61
9.1.2. Tarifas de acceso a los certificados 61
9.1.3. Tarifas de acceso a la información de estado o revocación 61
9.1.4. Tarifas para otros servicios 61
9.1.5. Política de reembolso 61

9.2. Responsabilidad financiera 61
9.2.1. Seguro de responsabilidad civil 61
9.2.2. Otros activos 61
9.2.3. Seguros y garantías para entidades finales 61

9.3. Confidencialidad de la información 62
9.3.1. Alcance de la información confidencial 62
9.3.2. Información no incluida en el alcance 62
9.3.3. Responsabilidad para proteger la información confidencial 62

9.4. Protección de datos de carácter personal 62
9.4.1. Plan de privacidad 62
9.4.2. Información tratada como privada 62
9.4.3. Información no considerada privada 62
9.4.4. Responsabilidad de proteger la información privada 62
9.4.5. Aviso y consentimiento para usar información privada 62
9.4.6. Divulgación conforme al proceso judicial o administrativo 62
9.4.7. Otras circunstancias de divulgación de información 63

9.5. derechos de propiedad intelectual 63

9.6. Obligaciones y garantías ... *63*
9.6.1. Obligaciones de la AC ... 63
9.6.2. Obligaciones de la AR ... 63
9.6.3. Obligaciones del suscriptor y del firmante ... 64
9.6.4. Obligaciones de las partes que confían ... 65
9.6.5. Obligaciones de otros participantes ... 65
9.7. Renuncia de garantías ... *66*
9.8. Limitaciones de responsabilidad ... *66*
9.9. Indemnizaciones ... *66*
9.9.1. Indemnización de la CA ... 66
9.9.2. Indemnización de los Suscriptores ... 66
9.9.3. Indemnización de las partes que confían ... 66
9.10. Periodo de validez de este documento ... *67*
9.10.1. Plazo ... 67
9.10.2. Terminación ... 67
9.10.3. Efectos de la finalización ... 67
9.11. Notificaciones individuales y comunicación con los participantes ... *67*
9.12. Modificaciones de este documento ... *67*
9.12.1. Procedimiento para las modificaciones ... 67
9.12.2. Periodo y mecanismo de notificación ... 67
9.12.3. Circunstancias bajo las cuales debe cambiarse un OID ... 67
9.13. Reclamaciones y resolución de disputas ... *67*
9.14. Normativa de aplicación ... *68*
9.15. Cumplimiento de la normativa aplicable ... *68*
9.16. Estipulaciones diversas ... *68*
9.16.1. Acuerdo íntegro ... 68
9.16.2. Asignación ... 68
9.16.3. Severabilidad ... 68
9.16.4. Cumplimiento ... 68
9.16.5. Fuerza Mayor ... 68
9.17. Otras estipulaciones ... *68*

Índice de tablas

Tabla 1 – Certificado de la AC FNMT raíz ... 15
Tabla 2 – Certificado de la AC subordinada ... 16
Tabla 3 – Perfil de la CRL ... 58

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 Firma Electrónica* y *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,* salvo el *Certificado de Firma de Código,* 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 siguientes *Certificados en el ámbito de la Administración:*

i. Certificado de Firma Electrónica

- *Certificado de Empleado Público*
- *Certificado de Empleado Público en QSCD nivel medio*
- *Certificado de Firma de Empleado Público en QSCD nivel alto*
- *Certificado con Seudónimo*
- *Certificado con Seudónimo de la Administración de Justicia*
- *Certificado de Firma Centralizada para Empleado Público*
- *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*

ii. Certificado de Sello Electrónico:

- *Certificado de Sello Electrónico para la Administración*

iii. Certificado de Autenticación:

- *Certificado de Autenticación de Empleado Público en QSCD nivel alto*

iv. Certificado de Firma de Código

- *Certificado de Firma de Código para la Administración.*

13. El presente documento se denomina *"Políticas y Prácticas de Certificación de certificados de firma electrónica y 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. Adicionalmente para los *Certificados de Firma Centralizada* se atenderá a lo dispuesto en la *Política y Prácticas del servicio de firma en servidor* que establece el conjunto de reglas y procedimientos específicos seguidos por la FNMT-RCM para la prestación de su servicio de firma electrónica en servidor.

17. 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: 1.3.6.1.4.1.5734.3.17.1

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

Nombre: Política de Certificación de *Certificado de Empleado Público*

Referencia / OID[1]: 1.3.6.1.4.1.5734.3.17.2

Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

Nombre: Política de Certificación de *Certificado con Seudónimo de la Administración de Justicia*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.3

Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

Nombre: Política de Certificación de *Certificado con Seudónimo*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.4

Tipo de política asociada: QCP-n. OID: 0.4.0.194112.1.0

Nombre: Política de Certificación de *Certificados de Firma Centralizada* para *Empleado Público*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.5

Tipo de política asociada: QCP-n.-qscd OID: 0.4.0.194112.1.2

Nombre: Política de Certificación de *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.6

Tipo de política asociada: QCP-n.-qscd OID: 0.4.0.194112.1.2

Nombre: Política de Certificación de *Certificados de Empleado Público en QSCD nivel medio*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.7

Tipo de política asociada: QCP-n-qscd OID: 0.4.0.194112.1.2

Nombre: Política de Certificación de *Certificado de Autenticación de Empleado Público en QSCD nivel alto*

[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.

Referencia / OID: 1.3.6.1.4.1.5734.3.17.9

Tipo de política asociada: NCP+ OID: 0.4.0.2042.1.2

Nombre: Política de Certificación de *Certificado de Firma de Empleado Público en QSCD nivel alto*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.10

Tipo de política asociada: QCP-n-qscd OID: 0.4.0.194112.1.2

Nombre: Política de Certificación de *Certificado de Firma de Código*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.17

Versión: 1.7

Fecha de aprobación: 24/06/2024

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

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

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

18. El *Certificado de Empleado Público*, es el *Certificado de Firma Electrónica* emitido por la FNMT-RCM que vincula al *Firmante* con unos *Datos de verificación de Firma* y confirma, de forma conjunta:

- la identidad del *Firmante* (*Personal al servicio de la Administración Pública*), incluyendo en su caso, su número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado, y
- la identidad del *Suscriptor* del *Certificado*, donde el *Firmante* ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

19. Los *Certificados de Empleado Público en QSCD (uso para firma y/o autenticación)*, son los *Certificados de Empleado Público* cuyas claves, pública y privada, han sido generadas en un *dispositivo cualificado de creación de firma.*

20. *Certificado con Seudónimo*, es el *Certificado de Empleado Público* que vincula un seudónimo otorgado por la Administración al *Personal al servicio de la Administración Pública* correspondiente.

21. El *Certificado de firma centralizada* para el *Personal al servicio de la Administración Pública* así como el *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia,* son *Certificados de Firma Electrónica* orientados a la realización de firmas a distancia o en servidor, esto es, la generación de las *Claves pública y privada* no son generadas directamente en el navegador de Internet del *Firmante* o en otro dispositivo en su poder, y tampoco se descarga su *Certificado*, sino que se generan y se almacenan en un dispositivo cualificado de creación de firma de la FNMT-RCM. Asimismo, la firma electrónica se realiza

de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del *Firmante* al que se le ha expedido el *Certificado*.

22. 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*

23. 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

24. 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. *Firmantes*
4. *Suscriptores* de los *Certificados*
5. Partes que confían
6. Otros participantes

1.3.1. Autoridad de Certificación

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

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

Tabla 1 – Certificado de la AC FNMT raíz

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

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

Certificado de la AC subordinada	
Sujeto	CN = AC Sector Público, serialNumber = 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

Certificado de la AC subordinada	
Algoritmo de firma	RSA – SHA256
Identificador de clave	E7:04:EE:70:91:11:92:44:F9:0E:92:8F:56:43:1E:07:1D:BF:04:9C

1.3.2. Autoridad de Registro

26. La Autoridad de Registro realiza las tareas de identificación del solicitante, *Personal al servicio de la Administración*, 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*.

27. Podrán actuar como entidades de registro de FNMT-RCM aquellas Oficinas de Registro designadas por el órgano, organismo o entidad *Suscriptora* del *Certificado* con las que ésta suscriba el correspondiente instrumento legal para cubrir dicha finalidad.

1.3.3. Firmantes

28. Los *Firmantes* son las personas físicas, *Personal al servicio de la Administración*, que mantienen bajo su uso exclusivo los *Datos de creación de firma* asociados a dicho *Certificado*.

1.3.4. Suscriptores de los certificados

29. Los *Suscriptores* de los *Certificados de Firma Electrónica, Certificados de Sello y Certificados de Firma de Código* son la Administración, organismos y entidades públicas representadas a través de los diferentes órganos competentes.

1.3.5. Partes que confían

30. 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*.

1.3.6. Otros participantes

31. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

32. Los *Certificados de Firma electrónica* y 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".

33. Los *Certificados de Firma Electrónica* emitidos bajo esta *Política de Certificación* son expedidos al *Personal al Servicio de la Administración*. Estos *Certificados* son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad 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.

34. El ámbito de aplicación de los *Certificados con Seudónimo*, se emitirán a aquellas Administraciones que lo requieran en virtud de su uso para aquellas actuaciones que, realizadas por medios electrónicos, afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones en las que esté legalmente justificado el anonimato para su realización.

35. El ámbito de aplicación de los *Certificados* expedidos bajo las Políticas identificadas con la denominación *Certificados con Seudónimo de la Administración de Justicia* y *Certificados de Firma Centralizada con seudónimo de la Administración de Justicia* es, exclusivamente, para la Administración de Justicia.

36. 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*.

37. 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.

38. El *Certificado de Autenticación de Empleado Público en QSCD nivel alto*, permite garantizar electrónicamente y acreditar la identidad del *Firmante* ante servicios y aplicaciones informáticas. Por otro lado, estos certificados tienen en cuenta los requisitos de la política NCP+ según establece la norma europea EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

39. El *Certificado de Firma de Empleado Público en QSCD nivel alto,* puede utilizarse para la firma electrónica de cualquier información o documento.

40. El *Certificado de Empleado Público en QSCD nivel medio*, puede utilizarse como mecanismo de autenticación ante servicios y aplicaciones informáticas. Además de, poder utilizarse para la firma electrónica de cualquier información o documento.

1.4.2. Restricciones en el uso de los certificados

41. Constituyen límites de uso de los *Certificados de Autenticación, los Certificados de Firma Electrónica* las diferentes competencias y funciones propias de la Administración Pública *Suscriptora* (actuando a través del personal a su servicio en calidad de *Firmante* de los *Certificados*), de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización. La FNMT-RCM y la Administración, organismos y entidades públicas podrán fijar en los acuerdos o convenios, a través del documento de relación correspondiente o, si fuera procedente, en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

42. 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.

43. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados de Autenticación, los Certificados de Firma Electrónica y los Certificados de Firma de Código* 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.

44. 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. Para poder usar los *Certificados de Autenticación y los Certificados de Firma Electrónica* de *Personal al servicio de la Administración* de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica* y, la Administración actuante, adquirir la condición de *Suscriptor*.

45. 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.

46. 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*.

47. En cualquier caso, si un tercero desea confiar en la *Firma o Sello electrónicos* realizada 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*.

48. Los *Certificados de Autenticación* no están habilitados en operaciones que requieran no repudio de origen, por tanto, no deberá emplearse para la firma de trámites y documentos en los que se precisa dejar constancia del compromiso del firmante con el contenido firmado.

49. 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 - a excepción de los *Certificados de Firma de Código*.
- 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

50. 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

51. 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

52. 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

53. 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

54. 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 anualmente 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

55. 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 Empleado Público:* Es el *Certificado de Firma Electrónica,* que incorpora los datos identificativos de dicho Personal y de la Administración pública en la que presta servicio.
- *Certificado de Empleado Público en QSCD:* Es el *Certificado de Empleado Público* cuyas claves, pública y privada han sido generadas en un *Dispositivo cualificado de creación de firma.* A efectos de la presente DPPP son *Certificados de Empleado Público en QSCD.*
  - *Certificado de Autenticación de Empleado Público en QSCD nivel alto*
  - *Certificado de Firma de Empleado Público en QSCD nivel alto*
  - *Certificado de Empleado Público en QSCD nivel medio.*
- *Certificado de Firma Centralizada:* Es el *Certificado de Firma Electrónica* orientado a la realización de firmas en remoto o en servidor. Esto significa que la generación de las *Claves pública y privada* se generan y almacenan en un entorno seguro perteneciente a la FNMT-RCM, garantizándose en todo momento el control exclusivo del uso de dichas *Claves* por parte del *Firmante.* A efectos de la presente DPPP son *Certificados de Firma Centralizada*:
  - *Certificado de Firma Centralizada para Empleado Público*
  - *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*
- *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia:* Es el *Certificado de Firma Centralizada* cuyo *Firmante* pertenecerá siempre a la Administración de Justicia *y* que vincula los datos de validación de una persona física y confirma el seudónimo otorgado por la Administración de Justicia como medio de identificación y firma de conformidad 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
- *Certificado de Firma Centralizada para Empleado Público:* Es el *Certificado de Firma Centralizada* expedido al *Personal al servicio de la Administración*, que vincula los datos de validación de dicho personal, y confirma tanto su identidad como la de la Administración pública en la que presta servicio.

- *Certificado de Firma de Código*: Permite firmar software y garantizar la identidad del propietario y la integridad del código.
- *Certificado de Firma Electrónica:* A efectos de la presente DPPP, son los *Certificados* cualificados expedidos al *Personal al servicio de la Administración*, que vincula los datos de validación de dicho personal, y confirma tanto su identidad como la de la Administración pública en la que presta servicio. Son *Certificados de Firma Electrónica*:
  - *Certificado de Empleado Público*
  - *Certificado de Empleado Público en QSCD nivel medio*
  - *Certificado de Firma de Empleado Público en QSCD nivel alto*
  - *Certificado de Firma Centralizada para Empleado Público*
  - *Certificado con Seudónimo*
  - *Certificado con Seudónimo de la Administración de Justicia*
  - *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*
- *Certificado con Seudónimo: Es el Certificado de Firma Electrónica* que vincula los *datos de validación* de una persona física y confirma el seudónimo otorgado por dicha administración.
- *Certificado con Seudónimo de la Administración de Justicia:* Es el *Certificado de Firma Electrónica* que vincula los datos de validación de una persona física y confirma el seudónimo otorgado por la Administración de Justicia como medio de identificación y firma de conformidad 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
- *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.
- *Código de Activación:* es una clave alfanumérica utilizada para validar y activar una cuenta en el Portal de Gestión de Identidades.
- *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.
- *Dispositivo cualificado de creación de firma (QSCD):* dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014
- *Firmante*: *Personal al servicio de la Administración* que hace uso de sus *Datos de creación de firma.*
- *Organismo de supervisión:* organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el artículo 17 del Reglamento eIDAS.

- *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.
- *Política y Prácticas del servicio de firma en servidor:* Documento que establece el conjunto de reglas y procedimientos específicos seguidos por la FNMT-RCM para la prestación de su servicio de firma electrónica en servidor
- *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

56. 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

57. 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

58. 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

59. 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.

60. 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

61. 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

62. 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

63. 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*.

64. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificados de Firma Electrónica,* 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

65. 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).

66. El campo Common Name de los *Certificados de Firma Electrónica* define al *Personal al servicio de la Administración* al que se le ha expedido el *Certificado*.

67. El campo Common Name de los Sellos Electrónicos 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

68. Los *Certificados de Firma Electrónica* que la FNMT – RCM expida bajo las presentes Políticas de Certificación y Prácticas de Certificación Particulares haciendo uso de seudónimos, indicarán claramente esta característica, de conformidad con el Reglamento eIDAS y la normativa nacional aplicable.

69. Para los *Certificados de Sello Electrónico*, no se contempla el uso de seudónimos como forma de identificación del *Suscriptor* y el atributo CN contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado*.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

70. 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

71. El nombre distintivo (*DN*) asignado a los *Certificados* expedidos a un *Sujeto*, 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

72. 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

73. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados de Empleado Público, Certificados con Seudónimo ni Certificados con Seudónimo para la Administración de Justicia* expedidos bajo las presentes *Políticas de Certificación* y *Prácticas de Certificación Particulares*, que son generadas bajo el exclusivo control del *Firmante* y, en su caso, con la intervención de la *Oficina de Registro* correspondiente, y cuya custodia está bajo responsabilidad del *Personal al servicio de la Administración Pública*.

74. Para la expedición de los *Certificados de Empleado Público en QSCD*, se requerirá y comprobará que el *Solicitante*, *Personal al servicio de la Administración*, genere las *Claves pública y privada* en un dispositivo cualificado de creación de firma.

75. Para la expedición de los *Certificados de Firma Centralizada*, se requerirá que el *Solicitante*, *Personal al servicio de la Administración*, genere las *Claves pública y privada* en el sistema de la FNMT-RCM, después de haber sido registrado en el mismo y una vez validada dicha generación por parte de la *Oficina de Registro*, tras el proceso de acreditación de la identidad del citado *Solicitante* y recabada su voluntad.

76. Para los *Certificados de Firma Centralizada*, después de informar al *Solicitante* que se le va a expedir su *Certificado*, el sistema genera la pareja de *Claves*, de forma que la *Clave privada* queda almacenada y protegida, garantizando su uso bajo el control exclusivo del *Personal al servicio de la Administración*.

77. 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

78. 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*.

79. Las actividades de comprobación de la identidad del *Personal al servicio de la Administración*, *Solicitantes* de los *Certificados*, tanto de *Firma Electrónica* como de *Sello Electrónico*, 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.

80. 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*.

81. 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

82. 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 Firma Electrónica*. 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.

83. 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.

3.2.3.1. Comprobación directa mediante presencia física

84. Los *Solicitantes* de *Certificados de Firma Electrónica* deberán comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, con alguno de los medios de identificación admitidos en derecho conforme a la legislación nacional vigente, presentándose en la *Oficina de Registro* designada a tal efecto por el órgano, organismo o entidad pública *Suscriptora* de la que depende el personal a su servicio. Dicha *Oficina de Registro* es creada por la Administración *Suscriptora*, que notifica a la FNMT-RCM la relación de personas habilitadas para realizar estas actividades de Registro, de acuerdo con los procedimientos establecidos a tal efecto, así como cualquier variación en la estructura de dicha Oficina.

85. 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.

3.2.3.2. Comprobación utilizando medios de identificación electrónica

86. La FNMT-RCM expedirá el *Certificado de Firma Electrónica* sin necesidad de que el peticionario comparezca ante una Oficina de Registro si en el proceso de solicitud de dicho *Certificado*, el *Solicitante* se identifica utilizando un *Certificado cualificado de firma electrónica* perteneciente a alguno de los siguientes tipos:

- Un *Certificado de Empleado Público* expedido por la FNMT-RCM, o por un *Prestador de Servicios de Confianza* con el que se tenga un acuerdo a este fin, en la solicitud de:
  - *Certificado de Empleado Público*
  - *Certificado con Seudónimo de la Administración de Justicia*
  - *Certificado de Firma Centralizada para Empleado Público*
  - *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*
- Un *Certificado con Seudónimo de la Administración de Justicia* expedido por la FNMT-RCM en la solicitud de:
  - *Certificado con Seudónimo de la Administración de Justicia*
  - *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*
- Un *Certificado con Seudónimo* expedido por la FNMT-RCM en la solicitud de:
  - *Certificado con Seudónimo*
- Un *Certificado de persona física* expedido por la FNMT-RCM en la solicitud de:
  - *Certificado de Firma Centralizada con Seudónimo de la Administración de Justicia*

87. No obstante, solo se permitirá la solicitud telemática del *Certificado de Firma Electrónica* mediante el uso de los *Certificados* electrónicos relacionados en el apartado anterior si, en el momento de la solicitud, no se ha superado el plazo máximo establecido por la legislación vigente desde la personación e identificación física del *Suscriptor*.

3.2.3.3. Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional

88. No será necesaria la personación cuando a la *Oficina de Registro* del órgano competente de la Administración le conste la identidad u otras circunstancias permanentes de los solicitantes de los *Certificados* (identidad, vigencia del cargo y demás condiciones a incluir en el *Certificado*) en virtud de la relación preexistente entre dichos *Solicitantes* y la Administración donde prestan servicio, si queda garantizado que dichos *Solicitantes* (*Personal al servicio de la Administración*) han sido identificados mediante personación física (de conformidad con el proceso descrito en el párrafo anterior), y el período de tiempo transcurrido desde dicha personación física es menor de cinco años.

3.2.4. Información no verificada del Suscriptor

89. Toda la información incorporada al *Certificado* electrónico es verificada por la *Autoridad de Registro*.

3.2.5. Validación de la autorización

90. La Autoridad de Registro verifica que el *Solicitante* de un *Certificado de Firma electrónica* expedido bajo la presente DPPP ha sido previamente autorizado por el *Suscriptor* para llevar a cabo dicha solicitud.

91. Además, en el caso de los *Certificados de Sello Electrónico*, 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

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

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

94. 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

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

3.3.2. Renovación después de una revocación

96. 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

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

98. 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

99. El *Solicitante* de este tipo de *Certificados* solo puede ser *Personal al Servicio de la Administración*, que haya sido previamente autorizado por el *Suscriptor*.

4.1.2. Proceso de registro y responsabilidades

100. El Solicitante, *Personal al servicio de la Administración*, 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. En el caso de los *Certificados* de Sello Electrónico, 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.

101. 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.

102. El apartado 9.8 "Responsabilidades" 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

103. Para los *Certificados de Firma Electrónica*, el *Solicitante* aportará los datos que se le requieran, acreditará su identidad personal y su condición de *Personal al servicio de la Administración*. En el caso de la expedición de *Certificados de seudónimo*, la FNMT-RCM, a través de la *Oficina de Registro,* constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite. FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración.

104. En el caso de *Certificados de Firma Centralizada*, durante el proceso de acreditación de la identidad, el *Solicitante* suscribirá las condiciones de uso del *Certificado*, y se le dotará de unas credenciales de identificación y configurará un *Código de Activación*.

105. Si se trata de los *Certificados de Sello Electrónico*, 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*.

106. Para la emisión de *Certificados de Firma Electrónica*, la FNMT-RCM podrá identificar al *Solicitante*, de forma alternativa a la comparecencia en la *Oficina de Registro*, mediante el uso de un *Certificado de Firma Electrónica cualificado* expedido al *Personal al servicio de la Administración,* garantizando así la autenticidad de todos los campos a incluir en el *Certificado* a expedir, siempre que no hayan transcurrido más de cinco años desde que se procedió a la identificación del *Firmante*.

107. La FNMT-RCM, podrá acordar con las Administraciones, organismos y entidades públicas que así lo soliciten, la creación de Oficinas de Registro delegadas, con el fin de centralizar la realización de los procedimientos de registro con destino a otras Administraciones, vinculadas o dependientes, que no dispongan de medios suficientes para hacerlo en aplicación de las leyes sobre racionalización del gasto.

4.2.2. Aprobación o rechazo de la solicitud del certificado

108. En los *Certificados de Firma Electrónica,* una vez confirmadas la identidad del *Solicitante* y la vigencia del cargo o empleo por la *Oficina de Registro*, ésta procederá a validar los datos y a enviarlos firmados, junto con el código de solicitud recogido en la fase de solicitud.

109. Para los *Certificados de Firma Centralizada,* una vez confirmados los datos, el *Solicitante* queda registrado en el sistema de la FNMT-RCM para dotarle de sus credenciales de identidad completas. La generación de las claves se producirá una vez que el *Firmante* configure la contraseña de firma que protegerá las claves, y solicite la generación de su identidad de firma. Estas acciones se llevarán a cabo accediendo con un nivel de aseguramiento alto a la aplicación de solicitud del *Certificado* (Portal de Gestión de Identidades).

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

111. 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.

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

4.2.3. Tiempo en procesar la solicitud

113. La solicitud aprobada de los *Certificados de Firma Electrónica* es procesada automáticamente por el sistema, por lo que no hay establecido un tiempo para este proceso.

114. Para 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

115. 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*.

116. La emisión de *Certificados* 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.

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

118. 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.

119. 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 los datos de identificación del *Personal al servicio de la Administración Pública*. En el caso de la expedición de *Certificados* electrónicos de *Personal al servicio de la Administración Pública con seudónimos,* el atributo *CN* incluye dicho seudónimo. Y en el de los *Sello Electrónicos*, el atributo *CN* contiene la denominación del sistema o de la aplicación del proceso automático para el que se expide el *Certificado*

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

120. 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/

121. En el proceso de emisión de los *Certificados de Empleado Público en QSCD*, se comprobará que el dispositivo empleado para la generación de claves de autenticación y firma es un *Dispositivo cualificado de creación de firma* conforme al Reglamento eIDAS.

122. En el proceso de emisión de los *Certificados de Firma Centralizada*, se requiere que el *Solicitante* se identifique ante el sistema con las credenciales recibidas más un segundo factor de autenticación que será remitido a su dirección de correo electrónico[2] y, una vez verificada su identidad, deberá solicitar expresamente la emisión de su *Certificado de Firma Centralizada.* De esta forma, la infraestructura vincula de forma segura los datos de identificación proporcionados por el Solicitante, según se ha descrito en el apartado "4.1.2 Proceso de registro" del presente documento, con el proceso de generación de su *Certificado*.

123. En ese momento, el sistema generará en un HSM protegido las *Claves pública y privada,* y expedirá al *Personal al servicio de la Administración* el *Certificado de Firma Centralizada* solicitado. Así mismo, el sistema requiere que el *Solicitante* establezca su contraseña de firma que le será requerida para realizar las operaciones que usen su *Clave privada*. Esta contraseña no es conocida (ni almacenada) en ningún momento por el sistema de la FNMT-RCM.

4.3.2. Notificación de la emisión

124. Una vez emitido el *Certificado de Firma Electrónica y 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

125. 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.

4.4.2. Publicación del certificado por la AC

126. 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

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

[2] La FNMT-RCM podrá utilizar otros medios de comunicación para transmitir este segundo factor de autenticación, previa autorización del *Solicitante*, como por ejemplo el uso de teléfonos móviles cuyo número haya sido previamente acreditado.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada y uso del certificado

128. La FNMT-RCM no genera ni almacena las Claves Privadas asociadas a los *Certificados* expedidos bajo la presente Política de Certificación, con excepción de los *Certificados de Firma Centralizada*. Corresponde la condición de custodio y responsables sobre el control de las claves del *Certificado*, al *Personal al servicio de la Administración* y, para *Certificados de Firma Centralizada*, a la FNMT-RCM.

129. Estos *Certificados* son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad 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.

130. 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

131. Los terceros que confían en las *Firmas electrónicas* realizadas con las *Claves privadas* asociadas al *Certificado* se atendrán a las obligaciones y responsabilidades definidas en la presente *DPPP*.

4.6. RENOVACIÓN DEL CERTIFICADO

132. 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

133. 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

134. 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

135. 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

136. 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

137. 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

138. 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

139. 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

140. 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

141. 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

142. 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

143. 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

144. 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

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

4.7.6. Publicación del certificado renovado

146. 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

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

4.8. MODIFICACIÓN DEL CERTIFICADO

148. 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

149. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

150. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

151. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

152. No se estipula la modificación.

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

153. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

154. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

155. No se estipula la modificación.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

156. 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.

157. 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*.

158. 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

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

160. 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) Cancelación de las credenciales de identificación del *Firmante* cuando sean *Certificados de Firma Centralizada.*

l) Pérdida de la certificación de *Dispositivo cualificado de creación de firma* QSCD, cuando sean *Certificados de Firma Centralizada o Certificados de Empleado Público en QSCD.*

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

162. 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 se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*

- Que la revocación le haya sido solicitada a través de la *Oficina de Registro* correspondiente a la entidad u organismo *Suscriptor* siguiendo el procedimiento establecido para este tipo de *Certificados*
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que en las causas c) a e) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.

163. 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.

164. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma* 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

165. 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

166. 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.

167. 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

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

169. 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.

170. 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.

171. 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 Firma Electrónica,* el solicitante deberá presentarse en su *Oficina de Registro,* donde se acreditará su identidad, se validará su capacidad para revocar dicho *Certificado* y se consignará la causa de revocación. La Oficina enviará de forma telemática mediante la aplicación de registro los datos a la FNMT-RCM, y procederá a la revocación del *Certificado*.

b. 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.

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

173. Tan pronto la revocación sea efectiva, serán notificados a través de la dirección de correo electrónico:

a. El *Firmante* y solicitante de la revocación cuando se trate de un *Certificado de Firma Electrónica*

b. El *Representante del Suscriptor* que solicita la revocación cuando se trate de un *Certificado de Sello Electrónico*

174. 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.

175. 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

176. 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

177. 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

178. 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

179. 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 *Certificado*s 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

180. 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

181. 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

182. La comprobación en línea del estado de revocación de los *Certificados de Firma Electrónica y 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

183. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

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

4.9.13. Circunstancias para la suspensión

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

4.9.14. Quién puede solicitar la suspensión

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

4.9.15. Procedimiento para la petición de la suspensión

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

4.9.16. Límites sobre el periodo de suspensión

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

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. Características operativas

189. 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

190. 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

191. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

192. 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.

193. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado de Firma Electrónica* emitido por la FNMT-RCM cuando exista otro vigente a favor del mismo *Firmante* y mismo *Suscriptor,* y perteneciente a la misma *Ley de Emisión,* conllevará la revocación del primero obtenido. Lo anteriormente descrito no sucederá en el caso de *Certificados de Sello Electrónico.*

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

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

195. En los *Certificados de Firma Centralizada*, en el caso de pérdida de la contraseña que protege el acceso a dicha *Clave* por parte del *Firmante,* se deberá revocar dicho *Certificado* y solicitar la emisión de uno nuevo.

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

196. No estipulado.

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

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

5.1. CONTROLES DE SEGURIDAD FÍSICA

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

5.1.1. Ubicación de las instalaciones

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

5.1.2. Acceso Físico

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

5.1.3. Electricidad y Aire Acondicionado

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

5.1.4. Exposición al agua

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

5.1.5. Prevención y Protección contra incendios

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

5.1.6. Almacenamiento de Soportes

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

5.1.7. Eliminación de Residuos

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

5.1.8. Copias de Seguridad fuera de las instalaciones

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

5.2. CONTROLES DE PROCEDIMIENTO

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

5.2.1. Roles de Confianza

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

5.2.2. Número de personas por tarea

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

5.2.3. Identificación y autenticación para cada rol

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

5.2.4. Roles que requieren segregación de funciones

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

5.3. CONTROLES DE PERSONAL

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

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

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

5.3.2. Procedimientos de verificación de antecedentes

214. Véase el apartado correspondiente en la *DGPC*

5.3.3. Requisitos de formación

215. Véase el apartado correspondiente en la *DGPC*

5.3.4. Requisitos y frecuencia de actuación formativa

216. Véase el apartado correspondiente en la *DGPC*

5.3.5. Secuencia y frecuencia de rotación laboral

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

5.3.6. Sanciones por acciones no autorizadas

218. Véase el apartado correspondiente en la *DGPC*

5.3.7. Requisitos de contratación de personal

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

5.3.8. Suministro de documentación al personal

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

5.4. PROCEDIMIENTOS DE AUDITORÍA

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

5.4.1. Tipos de eventos registrados

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

5.4.2. Frecuencia de procesamiento de registros

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

5.4.3. Periodo de conservación de los registros

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

5.4.4. Protección de los registros

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

5.4.5. Procedimientos de copias de seguridad de los registros auditados

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

5.4.6. Sistemas de recolección de registros

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

5.4.7. Notificación al sujeto causante de los eventos

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

5.4.8. Análisis de vulnerabilidades

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

5.5. ARCHIVADO DE REGISTROS

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

5.5.1. Tipos de registros archivados

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

5.5.2. Periodo de retención del archivo

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

5.5.3. Protección del archivo

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

5.5.4. Procedimientos de copia de respaldo del archivo

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

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

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

5.5.6. Sistema de archivo

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

5.5.7. Procedimientos para obtener y verificar la información archivada

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

5.6. CAMBIO DE CLAVES DE LA AC

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

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

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

5.7.1. Gestión de incidentes y vulnerabilidades

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

5.7.2. Actuación ante datos y software corruptos

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

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

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

5.7.4. Continuidad de negocio después de un desastre

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

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

245. 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

246. 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

247. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

248. En relación con la generación de las *Claves* del *Suscriptor,* excepto para los *Certificados de Firma Centralizada*, 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 de:

   a. El *Personal al servicio de la Administración* para los *Certificados de Firma Electrónica*.

   b. El *Responsable de Operaciones de Registro* o la persona autorizada por este en el caso de los *Certificados de Sello Electrónico.*

249. Las *Claves privadas* asociadas a los *Certificados de Empleado Público en QSCD* son generadas y custodiadas en un *Dispositivo cualificado de creación de firma* que cumple con los requisitos enumerados en el anexo II del Reglamento eIDAS.

250. Las *Claves privadas* asociadas a los *Certificados de Firma Centralizada* son generadas y custodiadas por el módulo de activación de firma de la FNMT-RCM, de forma que el acceso a dichas *Claves* se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del *Firmante*.

6.1.2. Envío de la clave privada al suscriptor

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

252. Las *Claves privadas* asociadas a los *Certificados de Firma Centralizada* son generadas en un dispositivo de creación de firma bajo el control exclusivo del *Firmante*, donde quedarán custodiadas para su uso. No existiendo, tampoco en este caso, entrega de la *Clave privada* al *Firmante*.

253. 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

254. 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

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

6.1.5. Tamaños de claves y algoritmos utilizados

256. El algoritmo utilizado es RSA con SHA-256.

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

- Claves de la AC FNMT raíz: 4.096 bits.
- Claves de la AC Sector Público Subordinada*:* 4.096 bits.
- Claves de los *Certificados de Autenticación Electrónica, Certificados de Firma Electrónica y Sello Electrónico:* 2.048 bits.
- Claves de los *Certificados de Firma de Código:* 3.072 bits.

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

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

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

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

260. El *Certificado* de la AC FNMT raíz tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

261. El *Certificado* de la AC FNMT Subordinada que expide los *Certificados de Firma Electrónica y Sello Electrónico* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.

262. Los *Certificados de Empleado Público, Certificados de Empleado Público en QSCD nivel medio, Certificados con Seudónimo, Certificados con Seudónimo de la Administración de Justicia* y *Certificados de Sello Electrónico* tienen habilitado exclusivamente los usos de clave de cifrado, autenticación y firma

263. Los *Certificados de Firma de Empleado Público en QSCD nivel alto* tienen habilitado exclusivamente el uso de clave de firma.

264. Los *Certificado de Autenticación de Empleado Público en QSCD nivel alto* tienen habilitado exclusivamente el uso de clave de autenticación.

265. Los *Certificados de Firma Centralizada* tienen habilitado exclusivamente el uso de firma.

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

6.2.1. Estándares para los módulos criptográficos

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

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

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

6.2.3. Custodia de la clave privada

268. 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.

269. Las *Claves privadas* asociadas a los *Certificados de Empleado Público en QSCD* son generadas y custodiadas en un *Dispositivo cualificado de creación de firma* que cumple con los requisitos enumerados en el anexo II del Reglamento eIDAS

270. En cuanto a las *Claves privadas* correspondientes a los *Certificados de Firma Centralizada* expedidos a los usuarios finales (*Firmantes*), quedan custodiadas en los sistemas de la FNMT-RCM de forma que únicamente el *Firmante* puede acceder a su *Clave privada*. El acceso queda garantizado mediante el uso de sus credenciales de identificación y su contraseña de firma (únicamente conocidos por el *Firmante*), más un segundo factor de autenticación como es una contraseña de un solo uso.

6.2.4. Copia de seguridad de la clave privada

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

6.2.5. Archivado de la clave privada

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

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

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

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8. Método de activación de la clave privada

275. 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.

276. 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 pines en un esquema de uso simultaneo M de N (2 de 5).

277. Los mecanismos de activación y uso de las *Claves privadas* de los *Certificados de Firma Centralizada* de entidad final se basan en el uso, por parte del *Firmante*, de sus credenciales de identificación y su contraseña de firma (únicamente conocidos por él), más un segundo factor de autenticación como es una contraseña de un solo uso.

6.2.9. Método de desactivación de la clave privada

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

6.2.10. Método de destrucción de la clave privada

279. 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.

280. En el caso de las *Claves privadas* de los *Certificados de Firma Centralizada* de entidad final, éstas serán destruidas una vez agotado su periodo de uso o cuando finalice la relación de los *Firmantes* con la FNMT-RCM. En todo caso, la destrucción de las claves privadas, será precedida de la revocación del *Certificado de Firma Centralizada*.

6.2.11. Clasificación de los módulos criptográficos

281. 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

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

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

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

- *Certificado* de la AC FNMT raíz y su par de *Claves*: hasta el 1 de enero de 2030.
- El *Certificado* de la AC subordinada que expide los *Certificados de Firma Electrónica y Sello Electrónico* y su par de *Claves*: hasta el 31 de diciembre de 2029.
- Los *Certificados de Firma Electrónica* y su par de *Claves:* no superior a 3 años.
- Los *Certificados de Sello Electrónico* y su par de *Claves*: no superior a 3 años.
- Los *Certificados de Autenticación Electrónica* y su par de Claves: no superior a 3 años.
- Los *Certificados de Firma de Código* y su par de Claves: no superior a 1 año.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

284. 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 Autenticación, Certificados de Firma Electrónica y Sello Electrónico y Certificados de Firma de Código,* se generan durante la ceremonia de *Claves* de creación de dichas *Autoridades de Certificación*.

285. En cuanto a los datos de activación de las *Claves* de los *Certificados de Firma Centralizada,* son generados por el módulo de activación de firma en el mismo entorno protegido contra manipulaciones que el dispositivo de creación de firma del *Prestador de Servicios de Confianza*, garantizando que dicha generación sólo puede ser realizada bajo el exclusivo control del que será el *Firmante.*

6.4.2. Protección de datos de activación

286. 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 pines en un esquema de uso simultaneo M de N (2 de 5).

287. La contraseña que protege el acceso a la *Clave privada* del *Certificado de Firma Centralizada* es confidencial, personal e intransferible. Por tanto, el *Firmante*, que además necesita un segundo factor de autenticación para activar su *Clave privada*, es responsable de la protección de sus datos de activación.

6.4.3. Otros aspectos de los datos de activación

288. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

6.5.1. Requisitos técnicos específicos de seguridad informática

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

6.5.2. Evaluación del nivel de seguridad informática

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

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.6.1. Controles de desarrollo de sistemas

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

6.6.2. Controles de gestión de la seguridad

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

6.6.3. Controles de seguridad del ciclo de vida

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

6.7. CONTROLES DE SEGURIDAD DE RED

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

6.8. FUENTE DE TIEMPO

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

6.9. OTROS CONTROLES ADICIONALES

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

6.9.1. Control de la capacidad de prestación de los servicios

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

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

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

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

301. Los *Certificados de Firma Electrónica* 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 319 412-2 "Certificate profile for certificates issued to natural persons".

302. 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".

303. Los *Certificados de Autenticación Electrónica* son expedidos como NCP+ conforme a los estándar europeo EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates".

7.1.1. Número de versión

304. Los *Certificados de Autenticación Electrónica*, los *Certificados de Firma Electrónica y Sello Electrónico* son conformes con el estándar X.509 versión 3.

7.1.2. Extensiones del certificado

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

7.1.3. Identificadores de objeto de algoritmos

306. El identificador de objeto (OID) correspondiente al algoritmo criptográfico utilizado (SHA-256 with RSA Encryption) es 1.2.840.113549.1.1.11

7.1.4. Formatos de nombres

307. La codificación de los *Certificados de Autenticación Electrónica*, *Certificados de Firma Electrónica y 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.

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

7.1.5. Restricciones de nombres

309. 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

310. El identificador de objeto (OID) de la política del *Certificado de Autenticación Electrónica*, *Certificado de Firma Electrónica y 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

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

7.1.8. Sintaxis y semántica de los calificadores de política

312. 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"

313. 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

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

7.2.2. CRL y extensiones

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

Tabla 3 – Perfil de la CRL

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

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

7.3.2. Extensiones del OCSP

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

8. AUDITORÍAS DE CUMPLIMIENTO

8.1. FRECUENCIA DE LAS AUDITORÍAS

318. 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".

319. 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".

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

321. Periódicamente se elaborarán los correspondientes planes de auditorías que contemplarán como mínimo la realización de las siguientes acciones:

- Análisis de riesgos conforme a lo dictado en el Sistema de Gestión de la Seguridad de la Información: Una revisión anual y un análisis completo cada tres (3) años
- Revisión 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"
- Calidad: ISO 9001: Una parcial anual externa más una auditoría anual interna preparatoria y una total externa cada tres (3) años, para mantenimiento de la certificación.
- Protección de datos: Una cada dos (2) años interna a realizar por el Departamento de Sistemas de Información.

322. La *Autoridad de Certificación* que expide los *Certificados de Firma Electrónica y 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 319 412-2 "Certificate profile for certificates issued to natural persons" o ETSI EN 319 412-3

"Certificate profile for certificates issued to legal persons" respectivamente. La auditoría es realizada anualmente por una empresa externa acreditada.

- Una auditoría cada dos (2) años de los sistemas de información de la FNMT-RCM que emplea para la prestación de Servicios de Confianza y conforme a lo dictaminado en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).

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

8.2. CUALIFICACIÓN DEL AUDITOR

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

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

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

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

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

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

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

8.7. AUTOEVALUACIÓN

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

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

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

9.1.1. Tarifas de emisión o renovación de certificados

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

9.1.2. Tarifas de acceso a los certificados

332. No estipulado.

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

333. 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

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

9.1.5. Política de reembolso

335. 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

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

9.2.1. Seguro de responsabilidad civil

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

9.2.2. Otros activos

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

9.2.3. Seguros y garantías para entidades finales

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

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.3.1. Alcance de la información confidencial

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

9.3.2. Información no incluida en el alcance

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

9.3.3. Responsabilidad para proteger la información confidencial

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

9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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

9.4.1. Plan de privacidad

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

9.4.2. Información tratada como privada

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

9.4.3. Información no considerada privada

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

9.4.4. Responsabilidad de proteger la información privada

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

9.4.5. Aviso y consentimiento para usar información privada

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

9.4.6. Divulgación conforme al proceso judicial o administrativo

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

9.4.7. Otras circunstancias de divulgación de información

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. Obligaciones de la AC

353. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con la persona asociada al *Certificado*, y que actúa como *Firmante*, 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*.

354. 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.

355. 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

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

9.6.2. Obligaciones de la AR

357. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en este documento y en la *DGPC*, las *Oficinas de Registro* y/o el *Responsable de Operaciones de Registro* tienen la obligación de:

- Comprobar fehacientemente los datos referidos a la identidad y a la condición del cargo, puesto de trabajo, empleo o cualquier otro dato que refleje o caracterice la relación del Personal al servicio de la Administración Pública como *Firmante* del *Certificado*, con la Administración, organismo o entidad a la que presta sus servicios (*Suscriptor* del *Certificado*)
- El *Prestador de Servicios de Confianza*, a través del *Responsable de Operaciones de Registro* velará por el cumplimiento de los procedimientos aprobados por FNMT-RCM

en materia de identificación de los Solicitantes de los Certificados e informará a los usuarios de los Certificados sobre su adecuado uso, de conformidad con las condiciones de uso, las Políticas y Prácticas de Certificación y la normativa aplicable.

- No realizar registros o tramitar solicitudes de personal que preste sus servicios en una entidad diferente a la que representa, o sobre la que no se tiene potestad o competencia para actuar como Oficina de Registro, sin perjuicio de la creación de Oficinas de Registro centralizadas o de convenios entre administraciones para efectuar registros.
- No realizar registros o tramitar solicitudes de Certificados emitidos bajo estas políticas y cuyo Solicitante no haya sido autorizado por el *Responsable de Operaciones de Registro*
- No tramitar *Certificados con Seudónimo*, salvo para su uso en aquellas actuaciones que, realizadas por medios electrónicos, afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones en las que esté legalmente justificado el anonimato para su realización
- Solicitar la revocación del *Certificado* desde que se tenga conocimiento cierto de cualquiera de los hechos determinantes especificados en el apartado 4.9.1 de esta DPPP

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

9.6.3. Obligaciones del suscriptor y del firmante

359. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, el *Personal al servicio de la Administración Pública*, como *Firmante* del *Certificado,* y/o en su caso el *Suscriptor* de los mismos, tienen la obligación de:

- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro sea inexacto o incorrecto o no refleje o caracterice su relación, con el órgano, organismo o entidad en la que presta sus servicios; o, existan razones de seguridad que así lo aconsejen.
- Realizar un uso adecuado del *Certificado* en base a las competencias y facultades atribuidas por el cargo, puesto de trabajo o empleo como *Personal al servicio de la Administración Pública*.
- Comunicar al *Responsable de Operaciones de Registro*, cualquiera de los hechos determinantes especificados en el apartado 4.9.1 de esta DPPP, con el fin de iniciar los trámites de revocación su *Certificado*.

360. Además, la persona física asociada a los *Certificados de Empleado Público en QSCD y Certificados de Firma Centralizada*, que actúa como *Firmante,* debe cumplir las normas de seguridad relacionadas con la custodia y uso de la contraseña de firma, como dato confidencial, personal e intransferible que garantiza el acceso a sus *Claves privadas*. Por tanto, dicho *Firmante* debe observar las siguientes cautelas relacionadas con la contraseña de firma:

- Conservar su confidencialidad, evitando comunicarlo a otras personas.

- Memorizarlo y no anotarlo en ningún documento físico ni electrónico.
- Cambiarlo en el momento en que tenga sospechas de que pueda ser conocido por otra persona.
- Notificar a la FNMT-RCM cualquier posible pérdida de control sobre su Clave privada, al objeto de revocar su *Certificado de Firma Centralizada para Empleado Público* y sus Claves asociadas.
- Abstenerse de escoger una contraseña fácilmente deducible de sus datos personales o predecibles (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones del mismo carácter, etc.).
- Seguir la política de seguridad de la FNMT-RCM en relación con la composición de la contraseña, periodicidad de modificación del mismo, etc.
- Las firmas electrónicas se crean exclusivamente haciendo uso del *QSCD* que el *PSC* le facilite en cada caso.

361. Será responsabilidad del *Firmante* 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.

362. En todo caso, el *Firmante* no usará los *Datos de creación de firma* o claves privadas, asociados a su *Certificado* en los casos en los que éste haya expirado su periodo de vigencia, o los *Datos de Creación de Firma / Sello* del Prestador puedan estar amenazados y/o comprometidos y así se haya comunicado por el Prestador o, en su caso, el *Firmante* conociera, sospechara o hubiera tenido noticia de estas circunstancias. Si el *Firmante* contraviniera esta obligación, será responsable de las consecuencias de los actos, documentos o transacciones firmadas en estas condiciones, así como de los costes, daños y perjuicios que pudieran derivarse, para la FNMT-RCM o para terceros, en caso de utilizar el *Certificado* más allá de su período de vigencia.

363. Asimismo, será el *Firmante* quien deba responder ante los miembros de la *Comunidad electrónica* y demás *Entidades usuarias* o, en su caso, ante terceros del uso indebido del *Certificado*, o de la falsedad de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros. Será responsabilidad del *Firmante* el uso que realice de su *Certificado,* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* y no se hubiera producido la subrogación prevista en la ley.

9.6.4. Obligaciones de las partes que confían

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

9.6.5. Obligaciones de otros participantes

365. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

366. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

367. 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.

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

9.9. INDEMNIZACIONES

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

9.9.1. Indemnización de la CA

370. No estipulado.

9.9.2. Indemnización de los Suscriptores

371. No estipulado.

9.9.3. Indemnización de las partes que confían

372. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

374. 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

375. 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

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

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

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

9.12.2. Periodo y mecanismo de notificación

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

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

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

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA DE APLICACIÓN

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

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

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

9.16. ESTIPULACIONES DIVERSAS

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

9.16.1. Acuerdo íntegro

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

9.16.2. Asignación

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

9.16.3. Severabilidad

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

9.16.4. Cumplimiento

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

9.16.5. Fuerza Mayor

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

9.17. OTRAS ESTIPULACIONES

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