Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DECLARACIÓN GENERAL DE PRÁCTICAS DE CERTIFICACIÓN

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM / 4.3	01/04/2016
Revisado por:	FNMT-RCM / 4.3	08/04/2016
Aprobado por:	FNMT-RCM / 4.3	11/04/2016

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
		Declaración de Prácticas de Certificación (de todas las políticas de certificación de la FNMT-RCM)	FNMT-RCM
3.0	05/05/2009	Creación del documento	FNMT-RCM
3.1	04/01/2010	Actualización de aspectos relativos al servicio de sellado de tiempo	FNMT-RCM
3.2	22/06/2010	Se refleja una nueva cadena de confianza para la prestación de servicios de certificación para la Administración pública. Se incluyen nuevos controles de seguridad para el incremento de las garantías y confianza en los servicios. Se incluye un apartado específico para la identificación de la FNMT-RCM como Prestador de Servicios de Certificación.	FNMT-RCM
3.3	19/12/2011	Se incluye un apartado específico sobre la gestión de *Políticas de Certificación*	FNMT-RCM
3.4	20/01/2012	Se incluye una nueva redacción del párrafo 12.1 describiendo las condiciones de reventa de los servicios.	FNMT-RCM
3.5	02/07/2013	Se incluye la periodicidad de un año para la realización de auditorías conforme a la norma ETSI 101-456	FNMT-RCM

		Prohibición de emitir *Certificados* de CA a otras entidades distintas a FNMT-RCM Limitación a un máximo de 3 años del período de vigencia de los certificados de entidad final. Reordenación en un mismo apartado de aspectos sobre políticas. Eliminación de referencias a CA Firma Móvil por haberse dado de baja el servicio. Inclusión de AC Componentes Informáticos en la cadena de certificación de AC Raíz.	
4.0	17/06/2014	Se eliminan las referencias a los anexos que desaparecieron en la versión 3.5. Se alinean las definiciones de titular y firmante con la LFE. Se actualizan algunos enlaces a la nueva página web de Ceres. Revisión auditoría conforme WebTrust y ETSI Ampliación de vigencia máxima de los certificados a 5 años, conforme modificación de la LFE.	FNMT-RCM
4.1	16/02/2015	Inclusión del compromiso con los requisitos base definidos por el CA/Browser forum	FNMT-RCM
4.2	14/07/2015	Inclusión del compromiso con los requisitos definidos por la ETSI 101 456.	FNMT-RCM
4.3	11/04/2016	Incorporación de referencias a ACs Usuarios y Representación y eliminación de ACs APE y AC ISA.	FNMT-RCM

Referencia: DPC/DGPC0403/SGPSC/2016

Documento clasificado como: *Público*

ÍNDICE

Índice **3**

1. Introducción **7**

2. Objeto **8**

3. Identificación de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda **8**

4. Definiciones **9**

5. Identificación de la presente Declaración General de Prácticas de Certificación y estándares seguidos para su elaboración **19**

6. Disponibilidad de la información y forma de contacto **20**

7. Cadenas de certificación **20**

7.1. AC RAIZ FNMT-RCM *22*

8. Publicación y repositorios **23**

8.1. Listado de repositorios y controles de acceso *23*

8.2. Frecuencia de publicación *24*

9. Controles de seguridad, registro de eventos y auditorías **25**

9.1. Registro de eventos *25*
9.1.1. Tipos de eventos registrados 25
9.1.2. Protección de un registro de actividad 26
9.1.3. Procedimientos de copias de seguridad de los registros auditados 26
9.1.4. Sistemas de archivo de registros 26
9.1.5. Datos relevantes que serán registrados 26
9.1.6. Protección de archivos 27
9.1.7. Realización de copias de seguridad de los archivos 27
9.1.8. Obtención y verificación de la información archivada 27
9.1.9. Cambio de claves de la AC 28

9.2. Controles de seguridad física, de procedimientos y de personal *28*
9.2.1. Controles de Seguridad Física 28
9.2.1.1. Ubicación de las instalaciones 28
9.2.1.2. Situación del Centro de Proceso de Datos 28
9.2.1.3. Acceso Físico 29
9.2.1.4. Electricidad y Aire Acondicionado 30
9.2.1.5. Seguridad del cableado 30
9.2.1.6. Exposición al agua 30
9.2.1.7. Prevención y Protección contra incendios 30
9.2.1.8. Almacenamiento de Soportes 30
9.2.1.9. Recuperación de la información 30
9.2.1.10. Eliminación de Residuos 31
9.2.1.11. Copias de Seguridad fuera de las instalaciones 31

9.2.2. Controles de Procedimiento 31
9.2.2.1. Roles de confianza 32
9.2.3. Controles de Seguridad de Personal 32
9.2.3.1. Seguridad en la definición del trabajo y los recursos 32
9.2.3.2. Inclusión de la seguridad en las responsabilidades laborales 32
9.2.3.3. Selección y política de personal 33
9.2.3.4. Requisitos de contratación de terceros 33
9.2.3.5. Conocimientos, cualificación, experiencia y requerimientos acreditativos 33
9.2.3.6. Frecuencia y secuencia de rotación de tareas 33
9.2.3.7. Documentación proporcionada al personal 33
9.2.3.8. Acuerdos de confidencialidad 34
9.2.3.9. Términos y condiciones de la relación laboral 34
9.2.3.10. Comunicación de las incidencias de seguridad 34
9.2.3.11. Comunicación de las debilidades de seguridad 34
9.2.3.12. Comunicación de los fallos del software 35
9.2.3.13. Aprendiendo de las incidencias 35
9.2.3.14. Procedimiento disciplinario 35
9.2.3.15. Conductas inadecuadas 35
9.2.3.16. Aplicaciones que comprometen la seguridad 36
9.2.3.17. Actividades no permitidas 36
9.2.3.18. Denuncia obligatoria 36
9.2.3.19. Formación 36
9.2.3.20. Administración de usuarios 37

9.3. Controles de seguridad técnica 37
9.3.1. Gestión del ciclo de vida de las Claves del Prestador de Servicios de Certificación 37
9.3.1.1. Generación e instalación de las Claves del Prestador de Servicios de Certificación 37
9.3.1.2. Almacenamiento, salvaguarda y recuperación de los Datos de creación y verificación de Firma del Prestador de Servicios de Certificación 38
9.3.1.3. Distribución de las claves públicas del Prestador de Servicios de Certificación 38
9.3.1.4. Período de uso de los Datos de creación y de verificación de Firma 38
9.3.1.5. Usos de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación 38
9.3.1.6. Cambio de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación 39
9.3.1.7. Fin del ciclo de vida de las Claves criptográficas del Prestador de Servicios de Certificación 39
9.3.2. Gestión del ciclo de vida de las Claves de los Titulares 39
9.3.2.1. Archivo de las claves públicas 40
9.3.2.2. Revocación de certificados 40
9.3.3. Ciclo de vida del hardware criptográfico utilizado para firmar Certificados 40
9.3.4. Datos de activación de las claves 41
9.3.5. Controles de seguridad de los componentes técnicos 41
9.3.6. Controles de seguridad de la red 41
9.3.7. Controles de ingeniería del módulo criptográfico 42
9.3.8. Niveles de seguridad 42
9.3.9. Procesos de auditoría y monitorización del sistema 42
9.3.10. Restablecimiento de los servicios en caso de fallo o desastre 42
9.3.11. Actualización de algoritmia 43
9.3.12. Terminación de la actividad de la FNMT-RCM como Prestador de Servicios de Certificación 43
9.3.13. Control de la capacidad de prestación de los servicios 43

9.4. Auditorías 43

9.4.1. Protección de las herramientas de auditoría 44
9.4.2. Identidad del auditor 44
9.4.3. Resultados de la auditoría y acciones correctivas 44
9.4.4. Comunicación de los resultados 45
9.4.5. Plan de auditorías 45
9.4.6. Procedimiento de análisis de vulnerabilidades 46
9.4.7. Procedimiento de notificación ante la detección de incidentes 46

10. Condiciones generales de los servicios de certificación 46

10.1. Gestión de las Políticas de Certificación 46

10.2. Sobre la gestión de certificados electrónicos 48

10.3. Sobre el servicio de información y consulta sobre el estado de validez de los certificados 49

10.4. Sobre el servicio de sellado de tiempo 49

10.5. desarrollo de aplicaciones informáticas 49

10.6. Imparcialidad de operaciones 49

11. Gestión de incidentes, vulnerabilidades y cese de la actividad 50

11.1. Gestión de incidentes y vulnerabilidades 50

11.2. Cese de la actividad del Prestador de Servicios de Certificación 50

11.3. Procedimiento de actuación ante la vulnerabilidad de los datos de creación de firma 51

11.4. Cambio de los Datos de creación de Firma de la FNMT-RCM 51

12. Perfil de los certificados 51

12.1. Restricciones de los nombres 51

12.2. Uso de la extensión Policy Constrains 52

12.3. Sintaxis y semántica de los Policy Qualifiers 52

12.4. Tratamiento semántico de la extensión "Certificate Policy" 52

13. Tarifas 52

14. Responsabilidades financieras 52

15. Datos de Carácter Personal 53

15.1. Información al Suscriptor 54

15.2. Información a la Entidad usuaria 55

15.3. Documento de seguridad LOPD 56
15.3.1. Objetivo y presentación del Documento de Seguridad LOPD 56
15.3.2. Normas y estándares 57
15.3.3. Principios y normas de obligado cumplimiento 57
15.3.4. Proceso de revisión 63

16. Propiedad Intelectual e Industrial 63

16.1. Prestación de servicios de validación de certificados para el tramo mayorista 64

17. Orden de prelación 65

18. Ley aplicable, interpretación y jurisdicción competente 65

19. Prestación de Servicios de Certificación y Firma Electrónica sobre certificados propios 65

Anexo: Perfil del certificado raíz FNMT – RCM 66

1. INTRODUCCIÓN

1. La Fábrica Nacional de Moneda y Timbre, Real Casa de la Moneda, (en adelante FNMT-RCM), a través del Departamento CERES (CERtificación ESpañola), con el fin de proporcionar transacciones electrónicas seguras a través de la Red, ha construido desde 1996 la infraestructura necesaria para prestar servicios de certificación electrónica con las máximas garantías. Esta infraestructura se encuentra en la actualidad plenamente operativa y experimentada. No en vano, el Departamento CERES ha obtenido como *Prestador de Servicios de Certificación*, *Autoridad de Sellado de Tiempo*, así como desarrollador de un sistema operativo para tarjetas criptográficas, la Certificación de Calidad ISO 9001, siendo el primer *Prestador de Servicios de Certificación* español en conseguirlo.

2. Asimismo es de destacar la implicación en proyectos de adecuación a las series ISO 27000 y a la normativa de la European Electronic Signature Standardisation Initiative[1] (en adelante "EESSI") en colaboración con el Centro de Evaluación de las Tecnologías de la Información – Instituto Nacional de Técnica Aeroespacial.

3. El objetivo de la FNMT-RCM, a través de su Departamento CERES, es proporcionar a sus clientes la *Infraestructura de Clave Pública,* así como todo un catálogo de servicios, sobre los cuales puedan apoyarse los servicios de las administraciones y las empresas para dotarlos de seguridad y validez legal de manera sencilla y cómoda para el ciudadano. La FNMT-RCM procurará estos objetivos utilizando principalmente técnicas de cifrado (para lograr la confidencialidad de la información) y de firma electrónica, que garantizan la identidad del firmante y la integridad de la información intercambiada, siendo el esquema de firma electrónica adoptado, coherente con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la Firma electrónica, con la legislación nacional de transposición, así como con la normativa específica de la propia FNMT-RCM, que garantizan, bajo cumplimiento de una serie de requisitos tasados, la equiparación jurídica de la *Firma electrónica reconocida* con la firma manuscrita con el alcance establecido legalmente, y sin perjuicio de los efectos previstos para el resto de tipologías de firmas electrónicas

4. La FNMT-RCM lleva más de un siglo fabricando productos de alta seguridad y de especial sensibilidad como monedas y billetes. Pero también fabrica otros productos de seguridad como el DNI, pasaportes, sellos, papel para contratos oficiales, libros de registro, tarjetas inteligentes, etiquetas seguras, etc. tanto para el mercado nacional como para el internacional.

5. De esta forma, la FNMT-RCM continúa con su papel tradicional ofreciendo garantías públicas de seguridad a la sociedad española, aunque ahora también desde la perspectiva de Internet y las nuevas tecnologías, adaptándose a los nuevos tiempos y dando el salto cualitativo desde el documento físico al *Documento Electrónico,* caso del DNIe y del Pasaporte electrónico.

[1] Iniciativa desarrollada por el mandato dado por la Comisión Europea al Information & Communications Technologies Standard Board, quien ha puesto en marcha a través del Information Society Standardisation System del European Committee for Standardisation y el European Telecommunication Standards Institute.

2. OBJETO

6. El presente documento tiene por objeto la información pública de las condiciones y características de los servicios de certificación por parte de la FNMT-RCM como *Prestador de Servicios de Certificación*, recogiendo en concreto 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, suspensión y extinción de la vigencia de los *Certificados* 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*, bien sean estos emitidos por la propia FNMT-RCM o, en su caso, por terceros, indicando las particularidades de cada caso, así como las condiciones aplicables al uso del servicio y garantías ofrecidas
   - la gestión de las solicitudes de *Sellos de Tiempo*, que se ofrecen como parte de la prestación del *Servicio de sellado de tiempo*.

7. Además, en el presente documento se recogen los detalles del régimen de responsabilidad aplicable a los miembros de la Comunidad Electrónica, 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.

3. IDENTIFICACIÓN DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA

8. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, de aquí en adelante FNMT-RCM, con NIF Q2826004-J, es una entidad pública empresarial de las previstas en el artículo 43.1.b), de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, que, como organismo público, tiene personalidad jurídica pública diferenciada, patrimonio y tesorería propios, y autonomía de gestión en los términos de dicha ley.

9. Está adscrita al Ministerio de Hacienda y Administraciones Públicas, el cual, a través de la Subsecretaría Hacienda y Administraciones Públicas, ejercerá la dirección estratégica y el control de eficacia de la Entidad en los términos previstos en los artículos 43 y 59, de la Ley 6/1997, de 14 de abril, citada.

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

servicios a los que ha sido facultada y ha obtenido el reconocimiento del entorno privado en este nuevo sector que representa la certificación electrónica y las redes telemáticas abiertas, alcanzando un destacado puesto en la prestación de los servicios de certificación.

11. En el desarrollo de esta actividad la FNMT-RCM ha alcanzado la acreditación de su sistema de gestión de la calidad de acuerdo a la normativa ISO 9001, otorgado por AENOR e IQNET para la prestación de servicios de certificación de firma electrónica, de sellado de tiempo y de desarrollo de sistemas operativos criptográficos para tarjetas inteligentes.

    Asimismo ha acreditado sus *Políticas de Certificación* para la emisión de *Certificados Reconocidos* conforme al estándar europeo ETSI TS 101 456 y sus políticas para la prestación de servicios de *Sellado de Tiempo* conforme al estándar europeo ETSI 101 023. Ambas acreditaciones han sido realizadas a través de una entidad independiente y en el marco de un esquema de certificación.

4. DEFINICIONES

12. Para informarse sobre los conceptos básicos relacionados con la Criptografía, los *Prestadores de Servicios de Certificación* y las *Infraestructuras de Clave Pública*, puede hacerlo a través de la dirección http://www.ceres.fnmt.es

13. No obstante, a los efectos de lo dispuesto en la presente Declaración General de Prácticas de Certificación y, en su caso, las Declaraciones de Certificación Particulares dependientes de esta, únicamente cuando los términos comiencen con letra mayúscula y estén en cursiva, se entenderá por:

    - *Agentes de Fechado:* Prestador del servicio de Sellado de Tiempo.
    - *Agentes de OCSP:* Prestador del servicio de OCSP.
    - *AEPD:* "Agencia Española de Protección de Datos". Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Su finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación.
    - *Autoridad de Certificación* (AC o CA –en inglés-): Sistema de confianza, gestionado por un *Prestador de Servicios de Certificación*, responsable de emitir y revocar los certificados digitales o *certificados*, utilizados en la *firma electrónica*. Jurídicamente es un caso particular de *Prestador de Servicios de Certificación* y por extensión se denomina al prestador *Autoridad de Certificación*.
    - *Autoridad de Sellado de Tiempo (AST o TSA –en inglés-)*: Sistema de confianza, gestionado por un *Prestador de Servicios de Certificación*, responsable de emitir *Sellos de Tiempo*. Jurídicamente es un caso particular de *Prestador de Servicios de Certificación* y por extensión se denomina al prestador *Autoridad de Sellado de Tiempo*.
    - *BOE:* (o Diario Oficial "BOE") Diario Oficial editado y distribuido por el Boletín Oficial del Estado; Organismo público, adscrito al Ministerio de la Presidencia, encargado además, de editar y distribuir el Boletín Oficial del Registro Mercantil, de publicar repertorios, compilaciones de textos jurídicos, y de la ejecución de los trabajos

de imprenta de carácter oficial solicitados por Ministerios, organismos y otras entidades públicas.

- *C:* En el ámbito del presente documento, es una abreviatura del vocablo inglés "Country" cuyo significado en español es "País". El "País" es un atributo que forma parte del Nombre Distintivo (*DN*) de un objeto dentro de la estructura de directorio *X.500* utilizado para nombrar la entrada correspondiente al objeto.
- *Cadena de certificación*: Una lista ordenada de *Certificados* que contiene al menos un *Certificado* y el *Certificado raíz* de la FNMT-RCM, sirviendo los *Datos de verificación de Firma* contenidos en éste último para posibilitar la autenticación del *Certificado*.
- *Certificado*: Un certificado electrónico es un documento firmado electrónicamente por un *Prestador de Servicios de Certificación* que vincula unos datos de verificación de firma a un *firmante* y confirma su identidad. Las condiciones específicas de cada tipo de certificado emitido por la FNMT-RCM figuran en las políticas *de certificación* y prácticas particulares correspondientes. *Certificado raíz*: Certificado cuyo *Titular* es la FNMT-RCM y que, estando auto firmado, es decir, emitido haciendo uso de los *Datos de creación de Firma* vinculados a los *Datos de verificación de Firma* contenidos en el propio *Certificado*, se conforma como el último *Certificado* de la cadena de confianza de todos los *Certificados* emitidos por la FNMT-RCM.
- *Certificado reconocido*: Es el *Certificado* electrónico emitido por un *Prestador de Servicios de Certificación* cumpliendo los requisitos establecidos en la Ley 59/2003, de firma electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los *Solicitantes* y a la fiabilidad y las garantías de los servicios de certificación que preste.
- *Cifrado asimétrico*: Trascripción en símbolos, de acuerdo con una *Clave* de cifrado, de un mensaje cuyo contenido se quiere ocultar conforme a un algoritmo tal que, el conocimiento de la *Clave* de cifrado no es suficiente para descifrar la trascripción, siendo necesario el conocimiento de la correspondiente *Clave* de descifrado. El conocimiento de la *Clave* de cifrado no implica el conocimiento de la *Clave* de descifrado, ni viceversa.
- *Clave*: Secuencia de símbolos que controlan las operaciones de cifrado y descifrado.
- *Clave Privada*: Del par de *Claves* criptográficas correspondientes a un *Cifrado asimétrico*, aquella destinada a permanecer en secreto. Las *Claves Privadas* pueden constituir, en función de su generación y utilización, *Datos de creación de Firma*.
- *Clave Pública*: Del par de *Claves* criptográficas correspondientes a un *Cifrado asimétrico*, aquella destinada a ser divulgada. Las *Claves Públicas* pueden constituir, en función de su generación y utilización, *Datos de verificación de Firma*.
- *Cliente OCSP*: Herramienta necesaria para que las *Entidades usuarias* de Derecho Privado, y, en su caso, de Derecho público, puedan hacer peticiones *OCSP*. La FNMT-RCM facilitará una relación de productos de libre distribución, pero no suministrará *Cliente OCSP* dada su amplia disponibilidad en el Mercado.
- *CN:* Contracción de los vocablos ingleses "Common Name" cuyo significado en español es "Nombre Común". El "Nombre Común" es un atributo que forma parte del Nombre Distintivo (*DN*) de un objeto dentro de la estructura de directorio *X.500* utilizado para nombrar la entrada correspondiente al objeto.

- *Comunidad Electrónica (en adelante Comunidad Electrónica o personas y/o entidades usuarias)*: Conjunto de personas y *entidades usuarias* que se relacionan con *Certificados* entre sí, bajo el marco general de la presente *Declaración General de Prácticas de Certificación*, y particular de los correspondientes convenios y/o contratos que hayan suscrito, directamente o a través de representantes, con la FNMT-RCM.

  Tendrán también la consideración de miembros de la *Comunidad Electrónica* las personas y entidades que utilicen *Certificados* electrónicos de prestadores distintos a la FNMT-RCM cuando se relacionaran con otros miembros de la *Comunidad Electrónica*, siempre que se hubieran declarados reconocidos y/o equivalentes estos certificados por la FNMT-RCM, a través de los correspondientes acuerdos.

  La FNMT-RCM informará a través de las direcciones web establecidas en esta Declaración de los miembros integrantes de la *Comunidad Electrónica*, cuando se trate de Administraciones públicas y Organismos y/o entidades y organizaciones empresariales si no existiera pacto o disposición legal que lo impida.

- *Confidencialidad*: Cualidad que supone que la información no es accesible o no ha sido revelada a personas, entidades o procesos no autorizados.
- *Contrato* y *convenio*: Instrumentos jurídicos previstos en la legislación correspondiente y/o de acuerdo con la autonomía de la voluntad, en los que se formaliza la relación para la prestación de servicios por la FNMT-RCM. Queda incluido en la categoría los contratos de emisión (formularios), revocación, renovación de *certificados* correspondientes, así como la aceptación de las condiciones de uso y limitaciones de las que sean informados los miembros de la Comunidad Electrónica a través de sistemas electrónicos, informáticos y telemáticos con tal carácter.
- *CPD*: Centro de Proceso de Datos.
- *Criptografía*: Disciplina que abarca los principios, significados y métodos para la transformación de datos para, de esta manera, ocultar el contenido-información, impidiendo su modificación no detectada y/o prevenir su uso no autorizado.
- *Datos de creación de firma*: Son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear firmas electrónicas. A efectos prácticos de esta *Declaración de Prácticas de Certificación* siempre coincidirá, desde un punto de vista técnico, con una *Clave* criptográfica asimétrica *Privada*.
- *Datos de verificación de firma*: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar firmas electrónicas. A efectos prácticos de esta *Declaración de Prácticas de Certificación* siempre coincidirán, desde un punto de vista técnico, con una *Clave* criptográfica asimétrica *Pública.*
- *Declaración de Prácticas de Certificación*: Declaración puesta a disposición del público por vía electrónica y de forma gratuita, que la FNMT-RCM realiza en calidad de *Prestador de Servicios de Certificación* y en cumplimiento de lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica (artículo 19).
- *Declaración de Prácticas de Sellado de Tiempo*: Declaración puesta a disposición del público por vía electrónica y de forma gratuita, que la FNMT-RCM realiza en calidad de *Prestador de Servicios de Sellado de Tiempo*.
- *Directorio*: Repositorio de información que sigue el estándar X.500 del ITU-T.

- *Disponibilidad*: Cualidad de los datos o de la información, que implica su condición de disponible, esto es; la posibilidad de disponer de ella o la posibilidad de utilizarla o usarla.
- *Dispositivo seguro de creación de Firma (DSCF)*: Elemento que sirve para aplicar los *Datos de creación de Firma*, que cumple con los requisitos establecidos en las normas específicas de aplicación en España, así como las recogidas en el Anexo III de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la Firma electrónica y en la Decisión de la Comisión de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en citada Directiva 1999/93/CE.
- *DN*: Contracción de los vocablos ingleses "Distinguished Name" cuyo significado en español es "Nombre Distintivo". El "Nombre Distintivo" es la identificación univoca de una entrada dentro de la estructura de directorio *X.500.* El DN está compuesto por el nombre común (*CN*) de la entrada más una serie de atributos que identifican la ruta seguida dentro de la estructura del directorio *X.500* para llegar a dicha entrada.
- *Documento electrónico*: la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.
- *Documento Nacional de Identidad Electrónico (DNI*e). Es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.
- *Documento de Seguridad LOPD*: Documento cuyo objetivo es establecer las medidas de seguridad a implantar por la FNMT-RCM en el entorno del *Prestador de Servicios de Certificación*, para la protección de los datos de carácter personal contenidos en el Fichero de Usuarios de Sistemas Electrónicos, Informáticos y Telemáticos (EIT), regulado por la Orden EHA/2357/2008, de 30 de julio (BOE de 7 de agosto).

  Conceptos relacionados:

  - *Administrador de la Aplicación*: Personal encargado de implementar las políticas definidas por el *Responsable del Fichero* en la aplicación que contiene el Fichero de Usuarios de Sistemas EIT. Tendrá los accesos necesarios para conceder, alterar o anular el acceso autorizado sobre los datos o recursos, previa autorización de los mismos por el *Responsable de Seguridad*. Se encargará de comunicar las incidencias de seguridad que ocurran al *Responsable de Seguridad*.
  - *Auditor de Seguridad*: Personal encargado de revisar y evaluar los controles propuestos en este documento o cualquier otro referenciado. Elabora informes con el grado de cumplimiento y las discrepancias encontradas.
  - *Cesión o comunicación* (de datos): toda obtención de datos resultante de la consulta de un fichero, la publicación de toda o parte de la información contenida en un fichero, su interconexión con otros ficheros, y toda comunicación de datos realizada por una persona distinta del afectado.

- *Consentimiento* (del interesado): toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- *Encargado del Tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- *Personal de Seguridad Informática*: Personal encargado de coordinar y controlar las medidas definidas en este manual de seguridad en cuanto a *LOPD*. También se encarga tanto de mantener y revisar las incidencias que ocurran y realizar los informes sobre estas incidencias para remitirlos al *Responsable del Fichero*, a través del *Responsable de Seguridad*. Además por instrucción del *Responsable del Fichero,* facilitan las autorizaciones para que se lleven a cabo las solicitudes de altas, modificaciones o bajas de accesos a la aplicación donde están los datos del Fichero de Usuarios de Sistemas EIT y en caso de no estar de acuerdo con la solicitud la contrasta con el *Responsable de Seguridad* y el *Responsable del Fichero*.
- *Operador de backup*: Personal responsable de la realización de las copias de seguridad y su posterior etiquetado y almacenamiento de forma segura, que depende del Área de Explotación, del *Prestador de Servicios de Certificación* de la FNMT-RCM.
- *Responsable del Fichero (o del Tratamiento)*: Persona que decide sobre la finalidad, contenido y uso del tratamiento. Es el encargado de autorizar los accesos necesarios y definir la política que crea conveniente para la seguridad de los datos. También se encarga de revisar los informes periódicos de incidencias. Todo ello sin perjuicio de la consideración de la FNMT-RCM como responsable del fichero a los efectos de lo dispuesto en la normativa vigente en materia de protección de datos de carácter personal.
- *Responsable de Seguridad*: Encargado de coordinar y controlar las medidas que impone el *Documento de seguridad LOPD* en cuanto al Fichero de Usuarios EIT según *LOPD*. Dicha función recae en el Director de Sistemas de Información de la FNMT-RCM.
- *Usuarios de la Aplicación*: Personal que requiere los datos del Fichero de Usuarios de Sistemas EIT para desarrollar sus funciones. Los tipos de acceso serán diferentes en relación con el trabajo que se lleva a cabo. Los usuarios son empleados del *Prestador de Servicios de Certificación* de la FNMT-RCM y tienen acceso a la información dependiendo del nivel de autorización otorgado por el *Responsable del Fichero*.

- *EIT*: Técnicas y medios electrónicos, informáticos y telemáticos.
- *Entidad usuaria*: Aquella persona, entidad pública o privada que ha firmado un contrato o convenio con la FNMT-RCM para actuar en la *Comunidad Electrónica*.
- *Fechado digital:* Véase *Sellado de Tiempo*.
- *Fechado electrónico:* Véase *Sellado de Tiempo*.
- *Firma electrónica*: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

- *Firma electrónica avanzada*: Es aquella *Firma electrónica* que permite establecer la identi*dad* personal del *Suscriptor* respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al *Suscriptor,* como a los datos a que se refiere, y por haber sido creada por medios que éste puede mantener bajo su exclusivo control.
- *Firma electrónica reconocida*: Es aquella *Firma electrónica avanzada* basada en un *Certificado reconocido* y generada mediante un *Dispositivo seguro de creación de Firma*.
- *Firmante*: La persona física que posee un dispositivo de creación de firma y que actúa (realiza la firma) en nombre propio o en nombre de una persona jurídica a la que representa.
- *Función hash*: Una *Función hash* es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado "resumen" o "Hash" de los datos originales, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen *Hash* idéntico.
- *Hash*: Resultado de tamaño fijo que se obtiene tras aplicar una *Función hash* a un mensaje, con independencia del tamaño de este, y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
- *Hashing*: Aplicación de una *Función hash* a un conjunto de datos.
- *Hoster informático*: Prestador de servicios informáticos de alojamiento de aplicaciones y/o de datos de terceros, que permite la conectividad del destinatario del servicio con los mismos y el acceso a ellos por los usuarios.
- *Infraestructura de Claves Públicas* (PKI, *public key infrastucture*): Infraestructura capaz de soportar la gestión de *Claves Públicas* para los servicios de autenticación, cifrado, integridad y no repudio.
- *Integridad*: Cualidad que implica que el conjunto de datos que configura el mensaje no carece de ninguna de sus partes, ni ha sido incluida ninguna parte adicional. Desde el punto de vista de la información que esos datos pudieran implicar, supone una inalterabilidad tanto de contenido como estructural.
- *Ley de Emisión:* Conjunto de características técnicas y jurídicas de un determinado tipo de *Certificado* electrónico, de acuerdo con las *Políticas y Prácticas de Certificación* de aplicación y en los correspondientes contratos y/o convenios con los miembros de la *Comunidad Electrónica*, sobre la base de la autonomía de la voluntad.
- *Listas de Revocación (CRL; Certificate Revocation List)*: Lista donde figuran exclusivamente las relaciones de *Certificados* revocados y suspendidos. Su acceso puede se restringido o no dependiendo de las *Políticas de Certificación* en cuestión.
- *LOPD:* Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.
- *MD5:* Message Digest (algoritmo de resumen de mensajes) en su versión 5. Desarrollado por el R. Rivest en 1991 y publicada su descripción en la RFC 1321. El algoritmo consiste en tomar mensajes de longitud arbitraria y generar un resumen de

128 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para dotar de *Integridad* los documentos durante el proceso de *firma electrónica*.

- *Malware (Malicious software o Software malicioso):* Véase *Software malicioso*.
- *Manual del Sistema de Gestión de la Seguridad de la Información de la FNMT-RCM como Prestador de Servicios de Certificación*: También referido como *Manual de Seguridad de CERES o Manual de Seguridad*. Este manual contempla los procedimientos del Sistema de Gestión de la Seguridad de la Información del Departamento CERES de la FNMT-RCM al amparo de la norma *ISO 27001: Sistemas de Gestión de la Seguridad de la Información (SGSI).*
- *Navegador (navegador Web, browser)*: Programa que permite visualizar los contenidos de las *páginas Web* en Internet. También se conoce con el nombre de *browser*. Algunos ejemplos de *navegadores Web* o *browsers* son: Internet Explorer, Chrome y Mozilla Firefox.
- *Número de serie de Certificado*: Valor entero, único en el ámbito de cada *Autoridad de Certificación* de la FNMT-RCM, que está asociado inequívocamente con un *Certificado* emitido por ella.
- *OCSP (Online Certificate Status Protocol):* Protocolo informático que permite comprobar de forma rápida y segura el estado de validez de un *Certificado* electrónico.
- *Oficinas de Registro*: Oficinas instaladas por la FNMT-RCM, o por otra entidad siempre que medie convenio con la FNMT-RCM suscrito por dicha entidad o por su superior jerárquico administrativo, que se constituyen a fin de facilitar a los ciudadanos y empresas, tanto en el ámbito nacional como internacional, la presentación de solicitudes relativas a los *Certificados*, con la finalidad de realizar la confirmación de su identidad y la entrega de los correspondientes títulos acreditativos de las cualidades personales, facultades de representación y demás requisitos exigidos para el tipo de *Certificado* que se solicite.

  Cuando existan garantías suficientes para la confirmación de la identidad y demás datos personales necesarios para la gestión de *Certificados*, las operaciones de registro podrán tener carácter telemático.
- *OID (Object Identifier)*: Valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de *OID*.
- *Operación Manual a Explotación*: Secuencia de operaciones que encontrándose documentadas, son realizadas de forma manual por un operador de la FNMT-RCM.
- *OU*: Contracción de los vocablos ingleses "Organizational Unit" cuyo significado en español es "Unidad Organizativa". La unidad organizativa es un atributo que forma parte del Nombre Distintivo de un objeto dentro de la estructura de directorio *X.500*.
- *O:* En el ámbito del presente documento, es una abreviatura del vocablo inglés "Organization" cuyo significado en español es "Organización". La "Organización" es un atributo que forma parte del Nombre Distintivo (*DN*) de un objeto dentro de la estructura de directorio *X.500* utilizado para nombrar la entrada correspondiente al objeto.

- *PC/SC:* Contracción de los vocablos ingleses "Personal Computer/Smart Card" cuyo significado en español es "Computadores Personales/Tarjetas Inteligentes". Es una especificación desarrollada por el Grupo de Trabajo PC/SC para facilitar la interoperatividad necesaria para permitir que la tecnología de Tarjetas de Circuitos Integrados también conocida como Tarjetas Inteligentes puedan ser eficientemente utilizadas en entornos de computadores personales.
- *Persona jurídica:* Conjunto de personas agrupadas que constituye una unidad con finalidad propia, la cual adquiere, como entidad, capacidad jurídica y de obrar distinta de la de los miembros que la componen.
- *PIN*: Contracción de los vocablos ingleses "Personal Identification Number" cuyo significado en español es "Número de Identificación Personal". Es un conjunto de datos alfanuméricos conocidos únicamente por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- *PKCS (Public-Key Cryptography Standards)*: Estándares criptográficos de *Clave Pública* producidos por RSA Laboratorios, y aceptados internacionalmente como estándares.
- *PKCS#7* (Cryptographic Message Syntax Standard): Estándar criptográfico de *Clave Pública* producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define una sintaxis genérica para mensajes que incluyan mejoras criptográficas, tales como firma digital y/o cifrado.
- *PKCS#10* (Certification Request Syntax Standard): Estándar criptográfico de *Clave Pública* producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de certificado.
- *PKCS#11 (Cryptographic Token Interface Standard):* Estándar Criptográfico de Clave Pública producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define un interfaz de programación independiente de la tecnología de base, para utilizar tokens criptográficos (por ejemplo, tarjetas inteligentes criptográficas) como medio de autentificación.
- *Política de Certificación (particular):* Documento que establece el conjunto de reglas que indica la aplicabilidad de un determinado tipo de *Certificado* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.
- *Política de Sellado de Tiempo (particular)*: Documento que establece el conjunto de reglas que indica la aplicabilidad de un determinado tipo de *Sellado de Tiempo* a la *Comunidad Electrónica* y/o clase de aplicación con requisitos de seguridad comunes.
- *Práctica de Certificación (particular):* Documento en el que se recogen los procedimientos específicos seguidos por la FNMT-RCM para la gestión del ciclo de vida de un determinado tipo de *Certificado* así como otros servicios de certificación que pudieran estar incluidos en el alcance de dicha práctica. *Prestador de Servicios de Certificación (PSC)*: Es aquella persona física o jurídica que, de conformidad con la legislación sobre firma electrónica expide *Certificados* electrónicos, pudiendo prestar además otros servicios en relación con la *Firma electrónica*.
- *Prestador de Servicios de Sellado de Tiempo*: Es aquella persona física o jurídica que, de conformidad con la normativa sobre Sellado de Tiempo expide *Sellos de Tiempo* electrónicos.

- *ROA*: *Real Observatorio de la Armada*: Laboratorio del Real Instituto y Observatorio Astronómico de la Armada dependiente del Ministerio de Defensa y asociado al Centro Español de Metrología, adscrito al *Boureau Internacional de Pesas y Medidas* y designado por el RD 1308/1992 como depositario del Patrón de Nacional de Tiempo.
- *RSA*: Acrónimo de Ronald Rivest, Adi Shamir y Leonard Adleman inventores del sistema criptográfico de clave asimétrica referido (1977). Criptosistema de clave pública que permite el cifrado y la firma digital.
- *Sellado de Tiempo (Time Stamping en inglés)*: Consignación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones *Request For Comments*: 3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)",* que logra fechar el documento de forma objetiva. También se refiere como *Fechado Electrónico o Fechado Digital*.
- *Sello de tiempo (Time Stamp en inglés)*: Estructura de datos que consigna una fecha y hora de forma aneja a un documento electrónico mediante el empleo de los *Datos de Creación de Firma* de una *Autoridad de Sellado de Tiempo*, logrando que, de forma indubitada se pueda atribuir un momento temporal a la existencia de dicho documento electrónico.
- *Servicio de información y consulta sobre el estado de validez de los certificados*: Servicio prestado bajo demanda por la FNMT-RCM a los interesados que lo soliciten por el cual se proporciona información sobre el estado de los *Certificados* por los que el usuario se interesa. Este servicio se puede prestar a través de diversas interfaces (página web, OCSP, Directorio Seguro, etc.). La FNMT-RCM sólo prestará este servicio para determinadas *Autoridades de Certificación* y sus límites de uso, obligaciones y responsabilidades de las partes vendrán descritas en las correspondientes prácticas particulares del servicio.
- *Servicio de Fechado Digital*: Véase *Servicio de Sellado de Tiempo.*
- *Servicio de Fechado Electrónico*: Véase *Servicio de Sellado de Tiempo.*
- *Servicio de Sellado de Tiempo:* Servicio prestado bajo demanda por la FNMT-RCM a los interesados que lo soliciten, que basándose en las especificaciones Request For Comments: RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" y ETSI 101861 "Time stamping profile", data los documentos de forma objetiva logrando que, de forma indubitada se pueda atribuir un momento temporal a la existencia de un documento electrónico. La FNMT-RCM sólo prestará este servicio para determinadas entidades y sus límites de uso, obligaciones y responsabilidades de las partes vendrán descritas en las correspondientes políticas y prácticas particulares del servicio.
- *Servicio de Validación de Certificados*: Véase *Servicio de información y consulta sobre el estado de validez de los certificados.*
- *SHA-1*: Secure Hash Algorithm (algoritmo seguro de resumen –hash–). Desarrollado por el NIST y revisado en 1994 (SHA-1). El algoritmo consiste en tomar mensajes de menos de 2^{64} bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para dotar de *Integridad* a los documentos durante el proceso de firma electrónica.

- *Sistema criptográfico*: Colección de transformaciones de texto claro en *texto cifrado* y viceversa, en la que la transformación o transformaciones que se han de utilizar son seleccionadas por *Claves*. Las transformaciones son definidas normalmente por un algoritmo matemático.
- *Software malicioso* (del inglés Malware: Malicious software)*:* Cualquier programa, documento, mensaje o elemento del mismo, susceptible de causar daños y/o perjuicios a los usuarios.
- *Solicitante*: Persona física mayor de 18 años o menor emancipado, que previa identificación y, en su caso, con poder bastante, solicita una operación relativa a un *Certificado* en su nombre o por cuenta del *Titular* del mismo.
- *Sujeto pasivo tributario*: Abarcará en su conjunto tanto a las *Personas jurídicas,* como a las entidades carentes de personalidad jurídica a las que, sin embargo, la normativa tributaria considera "sujetos pasivos" a efectos fiscales. Quedarán excluidas de este concepto por lo tanto, las personas físicas.
- *SSCD (Secure Signature-creation Device):* Véase *Dispositivo seguro de creación de firma.*
- *Suscriptor*: Persona, órgano, organismo o entidad de la Administración Pública que suscribe los términos y condiciones de uso del servicio prestado por la FNMT – RCM.
- *Tarjeta criptográfica*: Soporte que contiene un microprocesador o chip y que constituye un dispositivo criptográfico empleado para la realización de *firma electrónica* con los *Datos de Creación de Firma* albergados en su interior. La Tarjeta Criptográfica puede ser un DSCF si cumple lo especificado en su definición.
- *Texto en cifra ("texto cifrado")*: Conjunto de signos, guarismos o letras convencionales, y que solo puede comprenderse conociendo la *Clave*, es decir, la secuencia de símbolos que controlan las operaciones de cifrado y descifrado.
- *Tiempo Universal Coordinado* o UTC (Coordinated Universal Time): Es el tiempo de la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Es la escala de tiempo sucesora de GMT y que, a diferencia de este, se basa en referencias atómicas.
- *Titular* (de un *Certificado*): Es la persona cuya identidad queda vinculada a los *Datos de verificación de firma* (Clave Pública) del *Certificado* emitido por el *Prestador de Servicios de Certificación*. Por tanto, la identidad del titular queda vinculada a lo firmado electrónicamente, como *Firmante*, utilizando los *Datos de creación de firma* (Clave privada) asociados al *Certificado*.
- *Triple-DES*: Sistema de cifrado simétrico que surge como una evolución del DES (Data Encryption Standard – estándar de cifrado de datos) descrito en el FIPS 46-3 (Federal Information Processing Standard) que desarrolla el DEA (data encryption algorithm – algoritmo de cifrado de datos) también definido en el estándar ANSI X9.32.
- *UIT (Unión Internacional de Telecomunicaciones)*: Organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones.
- *Unidad de Sellado de Tiempo (TSU –en inglés-):* conjunto de hardware y software gestionado de forma independiente y que en cada momento sólo tiene activa una clave de firma para la emisión de sellos de tiempo.

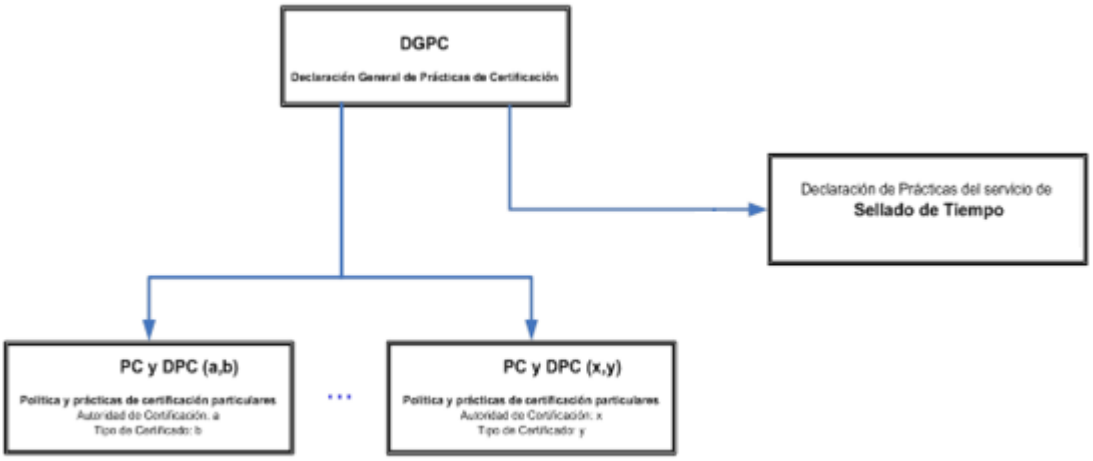
- *Usuario* (de un servicio): Persona que tiene derecho a usar las disposiciones de la FNMT-RCM en materia de los servicios de certificación en cuestión y con los límites y condiciones correspondientes al servicio en uso.
- *X.500*: Estándar desarrollado por la UIT que define las recomendaciones del Directorio. Se corresponde con el estándar ISO/IEC 9594-1. Da lugar a la serie de recomendaciones siguientes: X.501, *X.509*, X.511, X.518, X.519, X.520, X.521 y X.525.
- *X.509*: Estándar desarrollado por la UIT Para las *Infraestructuras de Clave Pública* y los llamados "certificados de atributos".

5. IDENTIFICACIÓN DE LA PRESENTE DECLARACIÓN GENERAL DE PRÁCTICAS DE CERTIFICACIÓN Y ESTÁNDARES SEGUIDOS PARA SU ELABORACIÓN

14. El presente documento se denomina "*Declaración General de Prácticas de Certificación de la FNMT-RCM*" e internamente será citado como "*Declaración General de Prácticas de Certificación*" o por su acrónimo "DGPC".

15. Este documento no trata los aspectos particulares de las diferentes *prácticas y políticas de certificación*, de validación o de sellado *de tiempo* que la FNMT-RCM implementa para la prestación de servicios de certificación. Dichas particularidades se desarrollan en los correspondientes documentos teniendo, como marco general de aplicación, la presente DGPC.

16. Las condiciones de uso, limitaciones, responsabilidades, propiedades y cualquier otra información que se considere específica de cada tipo de certificado, vendrán reflejadas en las Declaraciones de Certificación Particulares dependientes de esta DGPC. La estructura documental de las *políticas y prácticas de certificación* de los servicios de certificación de la FNMT-RCM se puede ver en la siguiente figura:



17. Esta DGPC se encuentra referenciada por el *OID* 1.3.6.1.4.1.5734.4 pudiendo ser localizada su última versión en vigor en la dirección

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

18. Estos procedimientos se basan principalmente en las normas del *European Telecommunications Standards Institute* (ETSI): ETSI TS 102 042, ETSI TS 101 456, ETSI TS 102 023, ETSI TS 101 733, ETSI TS 101 862 y ETSI TS 101 861.

6. DISPONIBILIDAD DE LA INFORMACIÓN Y FORMA DE CONTACTO

19. La FNMT-RCM interpretará, registrará, mantendrá, y publicará los procedimientos referidos en el apartado anterior "Identificación de la presente *Declaración General de Prácticas de Certificación* y estándares seguidos para su elaboración", pudiendo además recibir comunicaciones de los interesados sobre estos asuntos, a través de la siguiente dirección de correo electrónico: ceres@fnmt.es, y en el teléfono de atención al interesado: 902 181 696.

20. Para cuestiones organizativas o administrativas, la dirección de contacto de la FNMT-RCM como *Prestador de Servicios de Certificación* 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

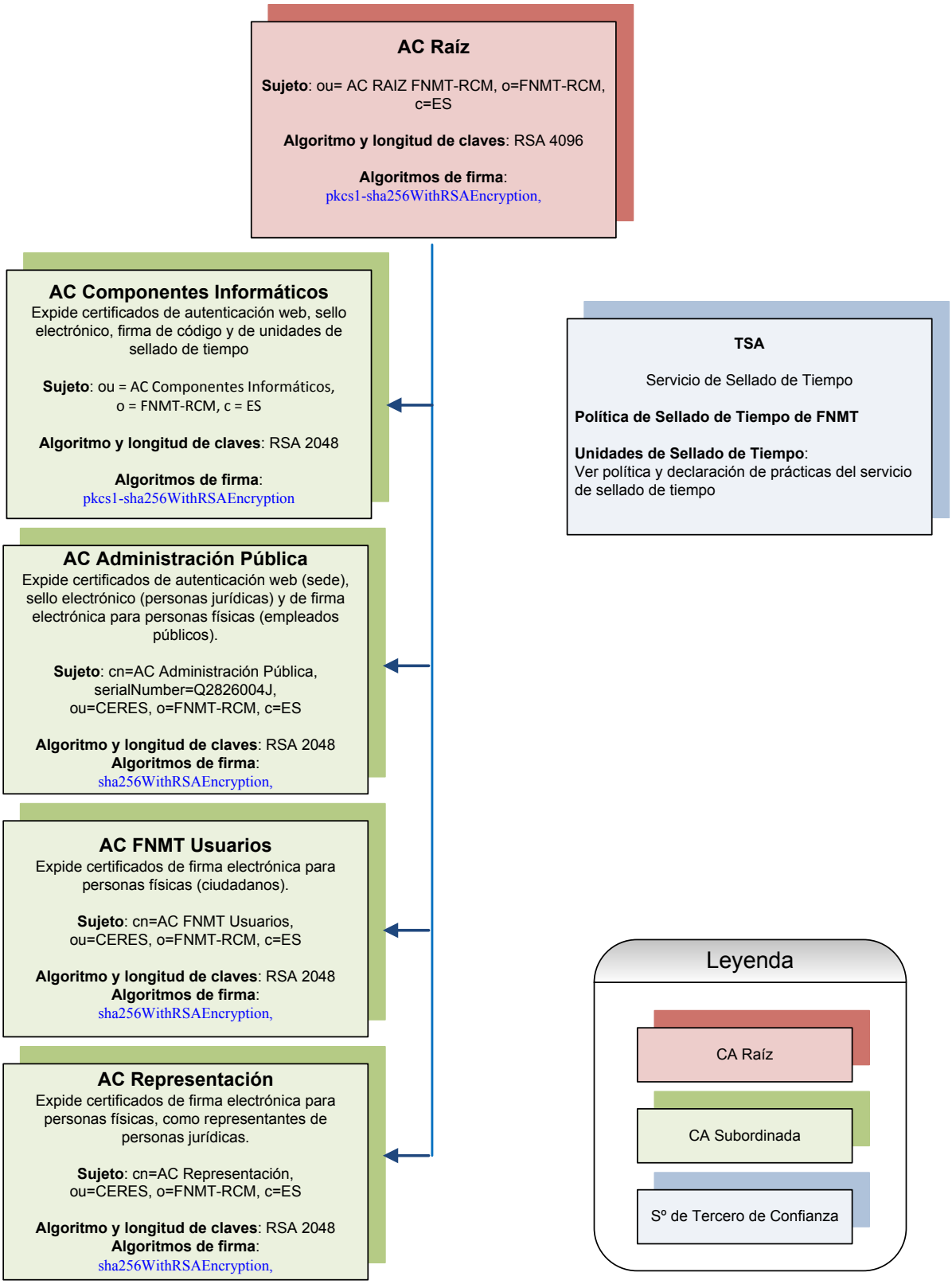
21. La FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación* cuando la legislación vigente así lo permita, contemple o lo requiera, recabará la dirección de correo electrónico, el número de teléfono móvil donde recibir mensajes de texto y del domicilio de los Titulares y/o *Suscriptores* en los contratos que presente a la firma de los *Solicitantes,* antes de emitir un *Certificado* o la contratación de un servicio en particular.

22. Esta información se recoge con la finalidad de prestar los servicios de confianza de los que son usuarios dichos Titulares y/o Suscriptores, y/o para notificar eventos de interés para el *Suscriptor* relacionados con los servicios de la FNMT-RCM y los *Certificados*, en especial, aquellos vinculados a las revocaciones y suspensiones de los *Certificados* o la resolución de los contratos que la FNMT-RCM haya celebrado con los *Suscriptores*. Asimismo dicha información se utilizará como canal de comunicación para cubrir cualquier necesidad en caso de contingencia de desastre que pudiera imposibilitar a la FNMT-RCM.

23. Será responsabilidad del *Solicitante* y posteriormente del *Suscriptor*, mantener la actualidad y veracidad de la mencionada información.

7. CADENAS DE CERTIFICACIÓN

24. Las *Cadenas de Certificación* empleadas por la FNMT-RCM como *Prestador de Servicios de Certificación* en el desempeño de sus funciones, los algoritmos de firma y sus parámetros son los siguientes:


AC Raíz
Sujeto: ou= AC RAIZ FNMT-RCM, o=FNMT-RCM, c=ES
Algoritmo y longitud de claves: RSA 4096
Algoritmos de firma: pkcs1-sha256WithRSAEncryption,
AC Componentes Informáticos
Expide certificados de autenticación web, sello electrónico, firma de código y de unidades de sellado de tiempo
Sujeto: ou = AC Componentes Informáticos, o = FNMT-RCM, c = ES
Algoritmo y longitud de claves: RSA 2048
Algoritmos de firma: pkcs1-sha256WithRSAEncryption
TSA
Servicio de Sellado de Tiempo
Política de Sellado de Tiempo de FNMT
Unidades de Sellado de Tiempo: Ver política y declaración de prácticas del servicio de sellado de tiempo
AC Administración Pública
Expide certificados de autenticación web (sede), sello electrónico (personas jurídicas) y de firma electrónica para personas físicas (empleados públicos).
Sujeto: cn=AC Administración Pública, serialNumber=Q2826004J, ou=CERES, o=FNMT-RCM, c=ES
Algoritmo y longitud de claves: RSA 2048
Algoritmos de firma: sha256WithRSAEncryption,
AC FNMT Usuarios
Expide certificados de firma electrónica para personas físicas (ciudadanos).
Sujeto: cn=AC FNMT Usuarios, ou=CERES, o=FNMT-RCM, c=ES
Algoritmo y longitud de claves: RSA 2048
Algoritmos de firma: sha256WithRSAEncryption,
AC Representación
Expide certificados de firma electrónica para personas físicas, como representantes de personas jurídicas.
Sujeto: cn=AC Representación, ou=CERES, o=FNMT-RCM, c=ES
Algoritmo y longitud de claves: RSA 2048
Algoritmos de firma: sha256WithRSAEncryption,
Leyenda
CA Raíz
CA Subordinada
Sº de Tercero de Confianza

25. La FNMT-RCM no utilizará sus *Datos de Creación de Firma* para emitir *Certificados* de *Autoridad de Certificación* a titulares distintos a ella o a cualquier tercero que lo pudiera solicitar.

26. Para la comprobación de la autenticidad de cualquier "*Certificado* autofirmado", elemento último de cualquier *Cadena de Certificación*, se puede verificar la huella digital correspondiente (en sus diferente formatos).

7.1. AC RAIZ FNMT-RCM

27. Por razones de interoperabilidad y previsiones de futuro, los *Datos de Creación de Firma* de esta *Autoridad de Certificación* han sido autofirmados con algoritmos diferentes dando lugar a tres *Certificados Raíz* correspondientes a "AC RAIZ FNMT-RCM". Así pues, se publica la siguiente información:

Algoritmo de Firma:

- pkcs1-sha1WithRSAEncryption[1],
- pkcs1-sha256WithRSAEncryption,
- pkcs1-sha512WithRSAEncryption

[1] Se publica por razones de interoperabilidad, para facilitar a los sistemas que no soporten pkcs1- sha256WithRSAEncryption/ pkcs1- sha512WithRSAEncryption la construcción de la cadena de confianza en los procesos de validación de certificados y firma.

Certificado pkcs1-sha1WithRSAEncryption

- Número de serie : 00 81 bb dd 6b 24 1f da b4 be 8f 1b da 08 55 c4
- Huella Digital (SHA-1) : b8 65 13 0b ed ca 38 d2 7f 69 92 94 20 77 0b ed 86 ef bc 10
- Huella Digital (MD5) : 0C:5A:DD:5A:AE:29:F7:A7:76:79:FA:41:51:FE:F0:35

Certificado pkcs1-sha256WithRSAEncryption

- Número de serie : 5d 93 8d 30 67 36 c8 06 1d 1a c7 54 84 69 07
- Huella Digital (SHA-1) : ec 50 35 07 b2 15 c4 95 62 19 e2 a8 9a 5b 42 99 2c 4c 2c 20
- Huella Digital (MD5) : E2:09:04:B4:D3:BD:D1:A0:14:FD:1A:D2:47:C4:57:1D

Certificado pkcs1-sha512WithRSAEncryption

- Número de serie : 0e 1c d8 cd 45 32 5a 47 00 51 0c aa c2 db 1e
- Huella Digital (SHA-1) : 14 4e 9a 4c d1 52 a9 47 5c dd 87 58 96 9c 13 e2 88 66 57 0e
- Huella Digital (MD5) : 8B:F1:A3:E2:DA:D9:61:99:AF:7F:73:3A:00:2E:DF:E0

8. PUBLICACIÓN Y REPOSITORIOS

8.1. LISTADO DE REPOSITORIOS Y CONTROLES DE ACCESO

28. La FNMT-RCM, como como *Prestador de Servicios de Certificación*, mantiene los siguientes repositorios de información:

a. *Declaración General de Prácticas de Certificación* y *Políticas* y *Prácticas de Certificación Particulares*. Acceso:

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

b. *Certificados* electrónicos de Autoridades de Certificación (accesible desde https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt)

i. Certificado de la AC RAIZ

ii. Certificado de AC Subordinada Administración Pública

iii. Certificado de AC Subordinada Componentes Informáticos

iv. Certificado de la AC Subordinada Representación

v. Certificado de la AC Subordinada Usuarios

c. Listas de Certificados Revocados:

i. AC RAIZ. Accesos:

1. ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

2. http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl

ii. AC Subordinada Administración Pública. Accesos:

1. ldap://ldapape.cert.fnmt.es/CN=CRL<xxx*>,CN=AC%20Administraci%F3n%20P%FAblica,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

2. http://www.cert.fnmt.es/crlsacap/ CRL<xxx*>.crl

iii. AC Subordinada Componentes Informáticos. Accesos:

1. ldap://ldapcomp.cert.fnmt.es/CN=CRL<xxx*>,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

2. http://www.cert.fnmt.es/crlscomp/CRLxxx.crl

iv. Certificado de la AC Subordinada Representación

1. ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>, OU=AC%20Representacion,OU=CERES,O=FNMT-

RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRL DistributionPoint

2. http://www.cert.fnmt.es/crlsrep/CRLnnn.crl

v. Certificado de la AC Subordinada Usuarios

1. ldap://ldapusu.cert.fnmt.es/CN=CRL<xxx*>, CN=AC%20FNMT%20Usuarios, OU=CERES, O=FNMT-RCM, C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

*xxx: número entero identificador de la CRL (CRL particionadas)

d. Servicio de comprobación del estado de revocación de certificados (OCSP):

i. AC RAIZ. Acceso:

http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

ii. AC Subordinada Administración Pública. Acceso:

http://ocspap.cert.fnmt.es/ocspap/OcspResponder

iii. AC Subordinada Componentes Informáticos. Acceso:

http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder

iv. Certificado de la AC Subordinada Representación

http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder

v. Certificado de la AC Subordinada Usuarios

http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder

29. Todos los repositorios anteriormente citados son de acceso universal, sin ningún control de acceso para la descarga de la información, salvo el acceso a los servicios de comprobación del estado de revocación de los certificados expedidos por la AC Subordinada Usuarios.

8.2. FRECUENCIA DE PUBLICACIÓN

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

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

9. CONTROLES DE SEGURIDAD, REGISTRO DE EVENTOS Y AUDITORÍAS

32. La FNMT-RCM dispone de procedimientos de control físico, lógico, de personal, y de operación, destinados a garantizar la seguridad necesaria en la gestión de los sistemas bajo su control e involucrados en la prestación de servicios de certificación. Asimismo, la FNMT-RCM registrará todos aquellos eventos relacionados con sus servicios que puedan ser relevantes, con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad se desarrollan de conformidad con la normativa aplicable para poder determinar las causas de una anomalía detectada.

33. A continuación y tomando como modelo de trabajo los documentos: *RFC 3647 Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework*, *ETSI 101 456 Policy requirements for certification authorities issuing qualified certificates y ETSI 102 023 Policy requirements for time-stamping authorities*, se muestran todos los controles implementados por la FNMT-RCM como *Prestador de Servicios de Certificación*, sin perjuicio de los de carácter confidencial y secreto de los que no se informa por razones de seguridad.

9.1. REGISTRO DE EVENTOS

9.1.1. Tipos de eventos registrados

34. La FNMT-RCM registrará todos aquellos eventos significativos con el fin de verificar que todos los procedimientos internos necesarios para el desarrollo de la actividad se ejecutan de acuerdo a este documento, a la normativa legal aplicable, y a lo establecido en el Plan de Seguridad Interna y en los Procedimientos de Calidad y Seguridad, y permitir detectar las causas de posibles anomalías.

35. Los eventos registrados serán todas aquellas operaciones que se realicen en la gestión de claves, gestión de *Certificados*, emisión de *Sellos de Tiempo*, información sobre el estado de *Certificados*, publicación, archivo, recuperación, directorio, registro de eventos, registro de usuarios y fabricación de tarjetas. La FNMT-RCM mantendrá archivados todos los eventos registrados más importantes, manteniendo su accesibilidad, durante un periodo nunca inferior a 15 años.

36. Todos los eventos registrados son susceptibles de auditarse.

37. Adicionalmente a los eventos expuestos, se guardarán todos los registros que especifica la norma ISO 9001 en la forma expuesta en los procedimientos generales de calidad de la FNMT-RCM, por un periodo no inferior a 3 años. Estos registros son, fundamentalmente:

- Registros de seguimiento de la Dirección.
- Registros de diseño, desarrollo y sus revisiones.
- Registro de Acciones Correctivas.
- Registro de satisfacción de clientes.
- Registro de las revisiones del sistema.
- Otros registros.

9.1.2. Protección de un registro de actividad

38. Una vez registrada la actividad de los sistemas los registros no podrán ser modificados, ni borrados, permaneciendo archivados en las condiciones originales.

39. Este registro tendrá sólo acceso de lectura, estando restringido a las personas autorizadas por la FNMT-RCM.

40. La grabación del registro, con el fin de que no pueda ser manipulado por nadie, se realizará automáticamente por el software específico que a tal efecto la FNMT-RCM estime oportuno.

41. El registro auditado, además de las medidas de seguridad establecidas en su grabación y posterior verificación, estará protegido de cualquier contingencia, modificación, pérdida y revelación de sus datos, durante su grabación en soportes externos, cambio de este soporte y almacenamiento de los mismos.

9.1.3. Procedimientos de copias de seguridad de los registros auditados

42. La FNMT-RCM, en su actividad de *Prestador de Servicios de Certificación*, por ser un sistema de alta seguridad, garantiza la existencia de copias de seguridad de todos los registros auditados.

9.1.4. Sistemas de archivo de registros

43. Los sistemas de archivos utilizados por la FNMT-RCM para conservar estos registros auditados, serán los internos propios de la infraestructura, y además se utilizarán soportes externos con capacidad de almacenamiento durante largos periodos de tiempo. Estos soportes tendrán las garantías suficientes para impedir que los registros sufran cualquier tipo de alteración.

44. La FNMT-RCM realizará varias copias que se almacenarán en diferentes lugares, que dispondrán de todas las medidas de seguridad física y lógica que eviten, en lo que razonablemente sea posible, una alteración del soporte almacenado y de los datos que contengan estos soportes. Cada copia será almacenada en un lugar diferente, con el objeto de prevenir posibles desastres en alguno de ellos.

45. Este archivo está provisto de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación de los certificados y eventos almacenados.

46. Todos los eventos almacenados contienen una marca de tiempo obtenida de la referencia temporal UTC (ROA). El Real Observatorio de la Armada (ROA), ostenta el patrón de tiempo oficial en España. La FNMT-RCM y el ROA han formalizado un acuerdo para la sincronización temporal de sus sistemas. Las condiciones del Sistema de Sincronismo quedan definidas en el documento "Sistema de Sincronismo FNMT – ROA".

9.1.5. Datos relevantes que serán registrados

47. Serán registrados:

- La emisión y revocación, y demás eventos relevantes relacionados con los *Certificados*, así como las operaciones relacionadas con la gestión de las claves y *Certificados* del *Prestador de Servicios de Certificación*
- Las *firmas*, y demás eventos relevantes relacionados con las *Listas de Revocación* (CRL's).
- Todas las operaciones de acceso al archivo de *Certificados*.
- Todas las operaciones de acceso a los *Servicios de Información Sobre el Estado de los Certificados*
- Eventos relevantes de la generación de pares de números aleatorios y pseudo-aleatorios para la generación de *Claves*.
- Eventos relevantes de la generación de pares de *Claves* propias o de soporte de autenticidad. En ningún caso se incluirán los propios números ni ningún dato que facilite su predicción.
- Todas las operaciones del servicio de archivo de *Claves* y del acceso al archivo de *Claves* propias expiradas.
- Todas las operaciones relacionadas con la actividad como tercera parte confiable.
- Los eventos relevantes de la operación de la *Autoridad de Sellado de Tiempo*, especialmente las correspondientes a la sincronización de relojes y pérdidas de sincronismo. Siempre se incluirá el momento exacto en el que se producen.

9.1.6. Protección de archivos

48. La FNMT-RCM garantiza que el archivo de eventos registrados cumple los siguientes requisitos:

- No podrá ser modificado por medios no autorizados.
- Ha de disponer de un alto grado de disponibilidad y fiabilidad.
- Se garantizará la confidencialidad de la información y quedará traza de los accesos realizados.

9.1.7. Realización de copias de seguridad de los archivos

49. En todo momento existirá una copia de seguridad de todos los archivos existentes en la FNMT-RCM, en su actividad como *Prestador de Servicios de Certificación*.

9.1.8. Obtención y verificación de la información archivada

50. El acceso al registro de archivos estará limitado al personal autorizado por la FNMT-RCM.

51. El acceso a datos cifrados por parte de terceras partes mediante el servicio de recuperación de datos sin autorización del usuario, deberá realizarse siempre bajo las condiciones que establezca la Ley y, en su caso, los *contratos* y *convenios* correspondientes.

9.1.9. Cambio de claves de la AC

52. Con anterioridad a la expiración del periodo de vigencia del certificado de la *Autoridad de Certificación* raíz, o de una *Autoridad de Certificación* subordinada, se procederá a la creación de la nueva *Autoridad de Certificación* raíz o subordinada correspondiente, mediante la generación de un nuevo par de claves. Las *Autoridades de Certificación* antiguas y sus claves privadas asociadas únicamente se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC.

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

53. En este apartado se describirán los controles no técnicos utilizados por la FNMT-RCM como *Prestador de Servicios de Certificación* para ejecutar de forma segura las funciones asociadas a la gestión de *Certificados*, los servicios de información sobre el estado de los *Certificados* y los servicios de *Sellado de Tiempo*.

9.2.1. Controles de Seguridad Física

54. La FNMT-RCM garantiza que cumple la normativa aplicable en todos los aspectos de seguridad física y las describe a lo largo del presente capítulo.

55. Se han establecido diferentes perímetros de seguridad, donde se llevan a cabo las actividades críticas o sensibles, con barreras de seguridad y con controles de entrada apropiados dotados de mecanismos de control de seguridad para reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

9.2.1.1. Ubicación de las instalaciones

56. El edificio donde se encuentra ubicada la infraestructura del *Prestador de Servicios de Certificación*, dispone de medidas de seguridad de control de acceso al edificio, de forma que el desarrollo de la actividad y prestación de los servicios se realicen con las suficientes garantías de *Confidencialidad* y seguridad.

9.2.1.2. Situación del Centro de Proceso de Datos

57. El CPD del *Prestador de Servicios de* Certificación ha sido construido atendiendo los siguientes requerimientos físicos:

- En un piso alejado de salidas de humos para evitar el posible daño que éste podría causar ante un posible incendio en las plantas superiores.
- Ausencia de ventanas practicables al exterior del edificio.
- Detectores de intrusión y cámaras de vigilancia en las áreas de acceso restringido para los períodos de tiempo en que los sistemas se encuentren desatendidos.
- Control de acceso basado en tarjeta y contraseña.
- Sistemas de protección y prevención de fuegos: campanas detectoras, extintores, formación de los operadores en la extinción de incendios, etc.

- Existencia de mamparas transparentes, limitando las distintas zonas, que permitan observar las salas desde pasillos de acceso, para detectar intrusiones o actividades ilícitas en el interior del CPD.
- Todo el cableado estará protegido contra daños o interceptación electromagnética o interceptación de la transmisión tanto de datos como de telefonía.
- Las instalaciones adscritas para la prestación de servicios de certificación se encuentran en el entorno de alta seguridad, separado del resto de actividades de la Entidad.

9.2.1.3. Acceso Físico

Perímetro de seguridad física

58. Una vez marcadas las áreas de seguridad donde se desarrolla la actividad FNMT-RCM como *Prestador de Servicios de Certificación*, se han establecido medidas físicas de control de accesos oportunas, sin olvidar que el recinto de la FNMT-RCM dispone de un avanzado sistema perimetral de seguridad física compuesto por diversos anillos con los adecuados medios técnicos y humanos, contando con la protección y vigilancia de las fuerzas y cuerpos de seguridad del Estado, así como de seguridad especializada.

59. Además de los diversos controles de acceso se dispone de diversos medios de control interior en las salas e instalaciones como son los controles de accesos basados en lectores de tarjetas, cámaras de videovigilancia, detectores de intrusismo, detectores de incendios, etc., además de los medios humanos dedicados a su atención tanto en el exterior como en el interior del recinto.

Controles físicos de entrada

60. Se dispone de un exhaustivo sistema de controles físicos de personas a la entrada y a la salida que conforman diversos anillos de seguridad.

61. Todas las operaciones críticas del *Prestador de Servicios de Certificación* se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

62. Estos sistemas estarán físicamente separados de otros sistemas de la FNMT-RCM, de forma que exclusivamente el personal autorizado del Departamento pueda acceder a ellos, y se garantice la independencia de otras redes de propósito general.

El trabajo en áreas seguras

63. El trabajo en áreas seguras se encuentra protegido por el control de acceso, y cuando el área así lo exige, monitorizado por el Departamento de Seguridad de la FNMT-RCM. No se permitirá, salvo autorización expresa de la Dirección, la presencia de equipos de fotografía, video, audio u otras formas de registro.

Visitas

64. El acceso de personas ajenas a la FNMT-RCM a sus instalaciones debe ser previamente comunicado al Departamento de Seguridad y autorizado por la Dirección del Departamento Ceres. Estas personas llevarán una identificación permanentemente visible y estarán en todo momento acompañadas por personal de la FNMT-RCM.

Áreas aisladas de carga y descarga

65. Las áreas de carga y descarga están aisladas y permanentemente vigiladas por medios técnicos y humanos.

9.2.1.4. Electricidad y Aire Acondicionado

66. Las salas donde se ubican las máquinas de la infraestructura del *Prestador de Servicios de Certificación*, disponen de suministro de electricidad y aire acondicionado suficiente para crear un entorno operativo fiable. Esta infraestructura productiva está protegida contra caídas de corriente o cualquier anomalía en el suministro eléctrico mediante una línea auxiliar independiente del centro de suministro principal, además de un grupo de suministro eléctrico autónomo.

67. Igualmente se han instalado mecanismos que mantienen controlados el calor y la humedad a sus niveles adecuados con el fin de conseguir una operación correcta del sistema del *Prestador de Servicios de Certificación*.

68. Aquellos sistemas que así lo requieren, disponen de unidades de alimentación ininterrumpida así como suministro eléctrico de doble proveedor y grupo electrógeno.

9.2.1.5. Seguridad del cableado

69. El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados (detectores en suelo y techo) para la protección del mismo ante incendios, así como sensores de humedad para detección precoz de fuga de líquidos.

9.2.1.6. Exposición al agua

70. Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado.

9.2.1.7. Prevención y Protección contra incendios

71. Las salas disponen de los medios adecuados (detectores) para la protección de su contenido ante incendios.

9.2.1.8. Almacenamiento de Soportes

72. La FNMT-RCM, como *Prestador de Servicios de Certificación*, establece los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

9.2.1.9. Recuperación de la información

73. Existen en la FNMT-RCM planes de copia de seguridad de toda la información sensible y de aquella considerada como necesaria para la continuidad del negocio del Departamento. Existen diversos procedimientos de elaboración y recuperación en función de la sensibilidad de la información y de los medios instalados.

9.2.1.10. Eliminación de Residuos

74. Se dispone de una política de gestión de residuos que garantiza la destrucción de cualquier material que pudiera contener información, así como una política de gestión de los soportes removibles.

9.2.1.11. Copias de Seguridad fuera de las instalaciones

75. No se realizan copias de seguridad aplicables a la FNMT-RCM como *Prestador de Servicios de Certificación* fuera de sus instalaciones.

9.2.2. Controles de Procedimiento

76. La FNMT-RCM procura que toda la gestión, tanto de procedimientos de operación, como administrativa, se lleve a cabo de forma confiable y conforme a lo establecido en este documento, realizando auditorías para evitar cualquier defecto que pueda conllevar pérdidas de confianza (a este respecto, puede consultarse el apartado "Auditorías").

- Se realizan auditorías, con el fin de comprobar el cumplimiento de las medidas de seguridad y de los requisitos técnicos y administrativos.
- Se realiza una segregación de funciones para evitar que una sola persona pueda conseguir el control total de la infraestructura. Para ello se definen múltiples perfiles asignados al personal de la infraestructura, entre los que se distribuyen las distintas tareas y responsabilidades.

77. La FNMT-RCM subcontrata ciertas actividades, como la del centro de atención a los usuarios de los *Certificados*. Estas actividades se desarrollan según lo establecido en las *Políticas y Prácticas de Certificación* de la FNMT-RCM y en los contratos y acuerdos formalizados con las entidades que realizan tales actividades. En estos casos, el acceso a la información propiedad de la FNMT-RCM por parte de terceros sigue el protocolo definido en la Política de Seguridad de esta entidad, en cuanto a la identificación de riesgos, establecimiento de controles de seguridad para proteger el acceso a la información y la formalización de los correspondientes acuerdos de confidencialidad y, si procede, el contrato para el tratamiento de datos de carácter personal en cumplimiento de la normativa vigente.

78. La FNMT-RCM establecerá programas de supervisión y control con el objeto de garantizar que las entidades que desarrollen funciones delegadas relacionadas con la prestación de servicios de certificación las realicen cumpliendo con las políticas y procedimientos de la FNMT-RCM.

79. La FNMT-RCM cuenta con un inventario actualizado de todos los activos de información y sistemas empleados para su tratamiento, detallando su propietario o responsable, naturaleza, clasificación y cualquier otro dato de interés para la prevención de incidentes y reacción ante estos. Existe una categorización de los sistemas de tratamiento de la información para el establecimiento de controles de seguridad conforme al Esquema Nacional de Seguridad.

80. La FNMT-RCM, a través de su Comité de Seguimiento del Código de Conducta, vela por el cumplimiento de las normas establecidas en dicho Código de Conducta para evitar situaciones que pudieran desembocar en un conflicto de intereses.

9.2.2.1. Roles de confianza

81. Las personas que desempeñan los "Roles de Confianza" están convenientemente formadas y tienen los conocimientos y experiencia necesarios para la ejecución de los trabajos vinculados a cada rol. Cuando así ha sido necesario, la FNMT-RCM ha proporcionado la formación técnica y de seguridad adecuada para el personal implicado en la gestión de sus sistemas confiables.

82. La identificación de los diferentes "Roles de Confianza", las tareas asignadas y los perfiles de seguridad quedan recogidos en el documento interno de la Dirección de Sistemas de Información de la FNMT – RCM definido como "Roles de Confianza y perfiles de seguridad". Los Roles de Confianza definidos son: Oficial de Seguridad, Administrador del Sistema, Operador del Sistema y Auditor del Sistema. La selección de las personas a las que se asignan estos roles se realiza teniendo en cuenta su formación, experiencia y los controles de Seguridad de Personal descritos a continuación.

9.2.3. Controles de Seguridad de Personal

9.2.3.1. Seguridad en la definición del trabajo y los recursos

83. La definición de los puestos de trabajo y sus responsabilidades, incluidas las de seguridad, se integran en el Convenio Colectivo que regula las relaciones de trabajo entre la FNMT-RCM y su personal laboral así como la normativa relativa a la función pública que resulte de aplicación.

9.2.3.2. Inclusión de la seguridad en las responsabilidades laborales

84. La seguridad está incluida en las responsabilidades laborales sin que precise mención adicional por ser la FNMT-RCM una entidad cuyo principal objetivo es la seguridad y por ende el objetivo y la responsabilidad de todos los miembros que la integran.

85. En cualquier caso, y sin perjuicio de la normativa pública correspondiente, preceptos del Código Penal que resulten de directa aplicación y cláusulas de determinados contratos del personal directivo, se encuentra específicamente incluida en capítulo XVII "Régimen disciplinario", artículo 63, las Faltas y Sanciones del referido Convenio Colectivo:

> *"Serán faltas graves:*
>
> *...*
>
> *13. La utilización o difusión indebida de datos o asuntos de los que se tenga conocimiento por razón del trabajo en el Organismo.*
>
> *...*
>
> *Serán faltas muy graves:*
>
> *...*
>
> *9. La utilización de información interna de la FNMT-RCM en beneficio propio o de empresas que entren en concurrencia con la FNMT-RCM.*
>
> *..."*

86. La sanción puede llegar al despido, con independencia de la conculcación que se haga de los preceptos del marco general legislativo y su correspondiente sanción o pena que instruyera la autoridad judicial.

87. Adicionalmente, en casos que así lo exijan, podrán existir acuerdos de confidencialidad personales a instancia de la FNMT-RCM y/o a petición de terceras partes.

9.2.3.3. Selección y política de personal

88. La selección y política de personal se integran en el Convenio Colectivo que regula las relaciones de trabajo entre la FNMT-RCM y su personal laboral, así como en la diversa normativa que le es de aplicación en virtud de la normativa relativa a la función pública y su Estatuto (Real Decreto 1114/1999, de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda y su condición de Entidad Pública Empresarial dependiente del Ministerio de Economía y Hacienda (actualmente Ministerio de Hacienda y Administraciones Públicas).

9.2.3.4. Requisitos de contratación de terceros

89. Las contrataciones de terceros realizadas por la FNMT – RCM están sometidas al Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público (LCSP). En este contexto, la Entidad es "poder adjudicador" y por tanto está sometida a la mencionada normativa, es decir, a una "regulación armonizada" de sus contrataciones. Para los casos en que no se aplique la LCSP, la FNMT-RCM empleará sus Instrucciones Internas de Contratación (IIC).

9.2.3.5. Conocimientos, cualificación, experiencia y requerimientos acreditativos

90. Los procedimientos para la gestión del personal de la infraestructura promoverán la competencia y el saber hacer de sus empleados, así como el cumplimiento de sus obligaciones.

91. Serán considerados puestos de confianza dentro del ámbito de este documento, aquellos que implican el acceso o el control de componentes que puedan afectar directamente a la gestión de los sistemas que implementan los servicios relacionados con los *Certificados*, la información sobre del estado de los *Certificados* y la emisión de *Sellos de Tiempo.*

9.2.3.6. Frecuencia y secuencia de rotación de tareas

92. No estipulado.

9.2.3.7. Documentación proporcionada al personal

93. A todos los empleados que tienen acceso o control sobre los sistemas confiables en los que se basan los servicios de tercero de confianza se les proporciona acceso a la Base de conocimiento del departamento, que recoge la documentación relativa a la normativa de seguridad, *Prácticas y Políticas de Certificación*, funciones encomendadas al personal, plan

de calidad y seguridad, política y planes de continuidad de negocio y, en particular, se proporciona la documentación precisa para desarrollar las tareas encomendadas en cada caso.

9.2.3.8. Acuerdos de confidencialidad

94. Todos los empleados, propios o contratados, que tienen acceso o control sobre los sistemas confiables en los que se basan los servicios de tercero de confianza, incluyendo el acceso restringido al *Directorio*, son considerados como empleados de confianza. Este personal incluye, pero no está limitado, a personal de servicio al cliente, personal administrador del sistema, personal de ingeniería, y ejecutivos que fueron nombrados para verificar la infraestructura de los sistemas de seguridad del *Prestador de Servicios de Certificación*.

95. El personal designado permanentemente o de forma temporal para estos puestos, será debidamente acreditado e identificado por la FNMT-RCM. Periódicamente se realizará un aseguramiento de que estas personas siguen teniendo la confianza de la FNMT-RCM para la realización de estos trabajos de confidencialidad.

96. Las relaciones entre terceras partes y la FNMT-RCM están protegidas por el correspondiente acuerdo de confidencialidad si en el transcurso de esta relación fuera necesario el intercambio de información sensible.

97. El personal de la FNMT-RCM, en virtud de su Convenio colectivo, no requiere la existencia expresa de acuerdos de confidencialidad personales, sin perjuicio de que en casos excepcionales puedan existir acuerdos de confidencialidad personales, normalmente a petición de terceras partes o a criterio de la propia FNMT-RCM.

9.2.3.9. Términos y condiciones de la relación laboral

98. Los términos y condiciones de la relación laboral se integran, además de en el contrato correspondiente, en el Convenio Laboral que regula las relaciones de trabajo entre la FNMT-RCM y su personal laboral, así como en la diversa normativa que le es de aplicación en virtud del mencionado Estatuto.

9.2.3.10. Comunicación de las incidencias de seguridad

99. Las incidencias son puestas en conocimiento de la Dirección con independencia de que se activen las oportunas acciones correctivas a través del Sistema de Gestión de Incidencias establecido en el Departamento para conducir a su solución de la forma más rápida posible según se describe en el "Procedimiento de Comunicación de Incidencias" y en el "Procedimiento de Gestión de Incidencias".

9.2.3.11. Comunicación de las debilidades de seguridad

100. Las debilidades de seguridad son clasificadas como incidencias, y como tales se resuelven, dando lugar a las oportunas acciones correctivas, según se describe en los procedimientos anteriormente mencionados.

9.2.3.12. Comunicación de los fallos del software

101. Los fallos del software son clasificados como incidencias y, como tales, se resuelven dando lugar a las oportunas acciones correctivas, según se describe en el "Procedimiento de Comunicación de Incidencias" y en el "Procedimiento de Gestión de Incidencias".

9.2.3.13. Aprendiendo de las incidencias

102. El "Procedimiento de Comunicación de Incidencias" y el "Procedimiento de Gestión de Incidencias" recogen también la agrupación y clasificación de las mismas para dar lugar a las correspondientes acciones correctivas o correctoras.

9.2.3.14. Procedimiento disciplinario

103. En el desarrollo de su actividad laboral para la FNMT-RCM, o siempre que usen medios y/o materiales de la FNMT-RCM, sus empleados, de conformidad con sus contratos de trabajo y/o la legislación aplicables, ceden exclusivamente, en toda su extensión, por toda la duración máxima prevista en la Ley y para el ámbito mundial a FNMT-RCM todos los derechos de explotación que pudieran corresponderles y en especial, y sin que esta enumeración se entienda con carácter limitativo, los derechos de reproducción, distribución, transformación y comunicación pública relativos a propiedad intelectual, así como demás derechos de propiedad industrial, o relativos a topografía de semiconductores, sobre los trabajo, obras, invenciones y creaciones que originen y/o desarrollen. El trabajador, como consecuencia de la cesión en exclusiva de los mencionados derechos sobre los trabajos, obras, invenciones y creaciones elaboradas o creadas como consecuencia de la relación laboral que les une con la FNMT-RCM o como consecuencia del uso de los medios materiales y/o técnicos de la FNMT-RCM, no gozará del derecho de explotar las citadas obras y/o creaciones de forma alguna, aunque ello no perjudicara a la explotación o uso de las mismas por parte de la FNMT-RCM.

104. Con el fin de lograr cumplir la normativa interna de la FNMT-RCM, las leyes y regulaciones aplicables y la seguridad de sus empleados, la FNMT-RCM se reserva el derecho a inspeccionar en cualquier momento y llevar un seguimiento de todos los sistemas informáticos de la FNMT-RCM.

105. Los sistemas informáticos sujetos a inspección incluyen, pero no se limitan, a los archivos de sistema de correo electrónico, archivos del disco duro de ordenadores personales, archivos de buzón de voz, colas de impresión, documentación obtenida del fax, cajones del escritorio y áreas de almacenado. Estas inspecciones se llevarán a cabo tras haber sido aprobadas por los Departamentos de Seguridad y Asuntos Legales, con los procedimientos establecidos en la normativa legal aplicable e intervención de los representantes sindicales, si procede. La FNMT-RCM se reserva el derecho de eliminar de sus sistemas informáticos cualquier material que considere ofensivo o potencialmente ilegal o fraudulento.

9.2.3.15. Conductas inadecuadas

106. La Dirección de la FNMT-RCM se reserva el derecho a revocar los privilegios de sistema de cualquier usuario en cualquier momento. No se permitirá conducta alguna que interfiera

con el ritmo habitual y adecuado de los sistemas informáticos de la FNMT-RCM, que impida a otros utilizar estos sistemas o bien que sea peligroso u ofensivo.

107. La FNMT-RCM no será responsable de las opiniones, actos, transacciones y/o negocios de fondo que los usuarios realizaran utilizando los servicios de certificación de la FNMT-RCM; todo ello sin perjuicio de la obligación de la FNMT-RCM de informar, si así lo conociera, a la autoridad competente.

9.2.3.16. Aplicaciones que comprometen la seguridad

108. Salvo concesión de la correspondiente autorización por parte de la Dirección de Sistemas de Información de la FNMT-RCM, los empleados de la FNMT-RCM no deberán adquirir, poseer, negociar o utilizar herramientas de hardware o software que pudieran ser empleadas para evaluar o comprometer los sistemas de seguridad informática. Algunos ejemplos de estas herramientas son: aquellas que ignoren la protección software contra copia no autorizada, detecten contraseñas secretas, identifiquen puntos de seguridad vulnerables y descifren archivos. Asimismo, sin el permiso adecuado, se prohíbe a los empleados utilizar rastreadores u otro tipo de hardware o software que detecte el tráfico de un sistema en red o la actividad de un ordenador, salvo en aquellos casos que su uso sea necesario para la realización de pruebas del sistema y previa comunicación al responsable del área.

9.2.3.17. Actividades no permitidas

109. Los usuarios no deben comprobar o intentar comprometer las medidas de seguridad de una máquina o sistema de comunicación a no ser que tal acción haya sido previamente aprobada, por escrito, por la Dirección de Sistemas de Información de la FNMT-RCM. Los incidentes relacionados con la "piratería informática", descubrimiento de contraseñas, descifrado de archivos, copia no autorizada de software, protección de datos de carácter personal y otras actividades que supongan una amenaza para las medidas de seguridad, o sean ilegales, se considerarán violaciones graves de la normativa interna de la FNMT-RCM. También está terminantemente prohibido el uso de sistemas de *bypass*, cuyo objetivo es evitar las medidas de protección, y otros archivos que puedan comprometer los sistemas de protección o los recursos.

9.2.3.18. Denuncia obligatoria

110. Todas las supuestas violaciones de la normativa, intrusiones en el sistema, afecciones por software malicioso y otras condiciones que supongan un riesgo para la información o los sistemas informáticos de la FNMT-RCM, deberán ser inmediatamente notificadas a la Dirección de Sistemas de Información.

9.2.3.19. Formación

111. La FNMT-RCM a través de su Centro de Formación, dependiente de la Dirección de Recursos Humanos, se encarga de gestionar el Plan Anual de Formación, con base en las necesidades generales de la empresa y las específicas de cada departamento. A este respecto, todos los empleados, propios o contratados, que tienen acceso o control sobre los sistemas confiables en los que se basan los servicios de tercero de confianza, son objeto del

citado Plan de Formación que, con carácter anual, viene a cubrir las necesidades de formación y concienciación en seguridad de la información, conforme al documento interno "Estándar de formación y sensibilización en seguridad de la información".

9.2.3.20. Administración de usuarios

112. La FNMT-RCM cuenta con procedimientos internos que establecen todos los controles necesarios para conocer las actividades que los usuarios realizan en los sistemas de información críticos que afectan a la provisión de Servicios de Certificación, con el fin de registrar cualquier incidencia producida y asegurar su trazabilidad. Para ello existe un registro auditable por cada acceso o intento de acceso fallido, tanto al sistema como a los activos del sistema. Todas las actividades relativas a funciones de seguridad son registradas.

113. Existe una política sobre la gestión de privilegios de acceso a la información y a los sistemas de información, así como de gestión de contraseñas de usuario. Los privilegios concedidos en el sistema a cada usuario son revisados periódicamente por el responsable de cada sistema o activo de información. Los privilegios relacionados con el acceso a aplicaciones críticas de la infraestructura del *Prestador de Servicios de Certificación* cuentan con un tratamiento especial, como el uso de certificados electrónicos en tarjetas criptográficas.

9.3. CONTROLES DE SEGURIDAD TÉCNICA

9.3.1. Gestión del ciclo de vida de las Claves del Prestador de Servicios de Certificación

9.3.1.1. Generación e instalación de las Claves del Prestador de Servicios de Certificación

114. Por motivos de seguridad y calidad, las *Claves* que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Certificación*, serán generadas por ella misma dentro de su propia infraestructura en un entorno físico seguro y al menos por dos personas autorizadas para ello.

115. La generación de las *Claves* y la protección de la *Clave Privada*, se realizan garantizando las necesarias medidas de confidencialidad, usando sistemas de hardware y software seguros y de confianza conforme a las normas EESSI CWA14167-1 y CWA14167-2, además de tomar las precauciones necesarias para prevenir su pérdida, revelación, modificación o su uso sin autorización, de acuerdo con los requisitos de seguridad especificados en las normas EESSI (en particular ETSI TS 101 456 y ETSI TS 102 023) aplicables a los *Prestadores de Servicios de Certificación*.

116. Los algoritmos y longitudes de *Clave* utilizados están basados en estándares ampliamente reconocidos para el propósito para el que son generadas.

117. Los componentes técnicos necesarios para la creación de *Claves* están diseñados para que una *Clave* sólo se genere una vez, y para que una C*lave Privada* no pueda ser calculada desde su *Clave Pública*.

9.3.1.2. Almacenamiento, salvaguarda y recuperación de los Datos de creación y verificación de Firma del Prestador de Servicios de Certificación

118. Los *Datos de creación de Firma* del *Prestador de Servicios de Certificación* se encuentran protegidos por un dispositivo criptográfico que cumple con los requisitos de seguridad FIPS PUB 140-2 Nivel 3. Las operaciones de firma de *Certificados, Listas de Revocación,* estructuras de datos relativas a la validez de los *Certificados y Sellos de Tiempo* son llevadas a cabo dentro del dispositivo criptográfico, que dota de *Confidencialidad* a los *Datos de creación de Firma* del *Prestador de Servicios de Certificación*.

119. Cuando los *Datos de creación de Firma* se encuentran fuera del dispositivo criptográfico, la FNMT-RCM aplica las medidas técnicas y organizativas apropiadas para garantizar su *Confidencialidad*.

120. Las operaciones de copia, salvaguarda o recuperación de los *Datos de creación de Firma* se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

121. Se mantiene una copia de los ficheros y componentes necesarios para la restauración del entorno de seguridad del dispositivo criptográfico, para el caso de que haya que hacer uso de ellos, en sobres de seguridad debidamente custodiados dentro de un armario ignífugo, que solo pueden ser obtenidos por personal autorizado.

9.3.1.3. Distribución de las claves públicas del Prestador de Servicios de Certificación

122. Los *Datos de verificación de Firma* del *Prestador de Servicios de Certificación* se distribuyen en un formato conforme a los estándares del mercado, pudiéndose consultar en la dirección www.cert.fnmt.es.

123. Para la comprobación de la autenticidad de cualquier "certificado autofirmado", elemento último de cualquier *Cadena de Certificación*, se puede verificar la huella digital correspondiente (en sus diferentes formatos, véase el apartado "*Cadenas de Certificación*").

9.3.1.4. Período de uso de los Datos de creación y de verificación de Firma

124. Los *Datos de creación y de verificación de Firma* del *Prestador de Servicios de Certificación* y de los *Titulares*, podrán utilizarse durante toda la vigencia del *Certificado* (sobre la vigencia de los *Certificados*, puede consultarse las correspondientes *Políticas y Prácticas de Certificación* particulares).

9.3.1.5. Usos de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación

125. Los *Datos de creación de Firma* de la *Autoridad de Certificación* de la FNMT-RCM serán utilizados única y exclusivamente para los propósitos de:

- Firma de *Certificados*.
- Firma de las *Listas de Revocación*.
- Firma de estructuras de datos relativas a la validez de los *Certificados*.

126. Adicionalmente, los *Datos de creación de Firma* de la FNMT-RCM en su actividad como *Prestador* de otros servicios de confianza, pueden ser utilizados para otros propósitos, como pueden ser:

- Firma de *Sellos de Tiempo*.
- Firma de documentos electrónicos distintos de los *Certificados* previstos en los fines y actividades de la FNMT-RCM, en los supuestos previstos en esta DGPC y en la normativa correspondiente.

9.3.1.6. Cambio de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación

127. La FNMT-RCM, en función de los avances ocurridos en materia criptográfica, estudiará el cambio de sus *Datos de creación y verificación de Firma*, cuando las circunstancias lo aconsejen y minimizando el impacto en su *Comunidad Electrónica*. En caso de optar por dicho cambio, la FNMT-RCM notificará a través del sitio www.cert.fnmt.es tal cambio en sus propios *Datos de creación y de verificación de Firma*. Adicionalmente, pondrá a disposición de los interesados los nuevos *Datos de verificación de Firma* en dicho sitio web.

9.3.1.7. Fin del ciclo de vida de las Claves criptográficas del Prestador de Servicios de Certificación

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

9.3.2. Gestión del ciclo de vida de las Claves de los Titulares

129. En su caso, la gestión del ciclo de vida de las *Claves* del *Titular* del *Certificado* se realizará conforme a lo definido en las *Políticas de Certificación y Prácticas de Certificación* particulares de cada una de las *Autoridades de Certificación* de la FNMT-RCM.

130. Sin perjuicio de lo que se establezca en los citados documentos de carácter particular, de forma general, la FNMT-RCM no almacenará las *Claves Privadas* de los *Titulares* que utilizan su infraestructura de servicios de certificación.

131. Las *Claves Privadas* de los *Titulares* son de uso y control exclusivo del propio *Titular* y generadas por éste, bien a través de *Dispositivos Seguros de Creación de Firma* o medios equivalentes.

132. La FNMT-RCM sólo conservará la *Clave Pública* del *Titular* y la prueba de posesión de la *Clave Privada* (*Clave Pública* o mensaje cifrado con la *Clave Privada*) según el ordenamiento legal vigente, durante un periodo no menor a 15 años.

133. El uso de las *Claves* de los *Titulares* se detalla en cada una de las diferentes *Prácticas de Certificación* Particulares cubiertas por la FNMT-RCM como *Prestador de Servicios de Certificación*.

134. Los *Datos de Creación de Firma* y los *Datos de Verificación de Firma* de los miembros de la *Comunidad Electrónica*, podrán utilizarse durante todo el periodo de vida del *Certificado*, pudiendo ser éste de hasta cinco años máximo. Véase a este respecto cada una de las

diferentes *Prácticas de Certificación Particulares* cubiertas por la FNMT-RCM como *Prestador de Servicios de Certificación*.

9.3.2.1. Archivo de las claves públicas

135. La FNMT-RCM conserva todas las claves públicas durante el periodo exigido por la legislación vigente, y en cualquier caso durante el periodo de tiempo en el que los servicios de certificación relacionados con los *Certificados* estén activos.

9.3.2.2. Revocación de certificados

136. La revocación de *Certificados* emitidos por la FNMT – RCM se realizará conforme a las *Políticas de Certificación y Prácticas de Certificación* particulares aplicables a cada *Certificado*.

137. En cuanto al plazo en el que la *Autoridad de Certificación* resuelve la solicitud de revocación, la FNMT – RCM procede a la revocación inmediata del certificado en el momento de verificar la identidad del firmante o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa.

La publicación de las *Listas de Revocación* (*CRL*) 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.

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

- la *Firma Electrónica* reconocida del *Prestador de Servicios de Certificación* emisor del *Certificado,*
- que el *Certificado* del *Suscriptor* continúa vigente y activo
- el estado de los *Certificados* incluidos en la *Cadena de Certificación.*

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

140. 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.

9.3.3. Ciclo de vida del hardware criptográfico utilizado para firmar Certificados

141. La FNMT-RCM dispone de los medios necesarios para asegurar que el hardware criptográfico utilizado para la protección de sus *Claves* como *Prestador de Servicios de Certificación:*

- No ha sido manipulado durante su transporte, mediante un proceso de inspección del material suministrado que incluye controles para detectar su autenticidad y posible manipulación.
- Funciona correctamente, mediante procesos de monitorización continua, inspecciones periódicas de mantenimiento preventivo y servicio de actualización de software y firmware.
- Permanece en un entorno físicamente seguro desde su recepción hasta su destrucción, llegado el caso.

9.3.4. Datos de activación de las claves

142. 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.

143. 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).

144. Los mecanismos de activación y uso de las claves privadas de los certificados de entidad final se basan en pines de acceso a los métodos de generación de claves privadas utilizados por el suscriptor, que en todo caso se mantienen bajo su estricto control y cuya custodia recae bajo su responsabilidad.

9.3.5. Controles de seguridad de los componentes técnicos

145. En la definición de la seguridad de todos los componentes técnicos que la FNMT-RCM utiliza en el desarrollo de su actividad como *Prestador de Servicios de Certificación*, así como en su estructura y procedimientos, se tienen presente en todo lo relativo a la certificación de la seguridad de los Sistemas de Información, de acuerdo al Esquema Nacional de Certificación de la Seguridad de los Sistemas de Información, que se aprueben en España, en particular los relativos a EESSI que sean publicados en el Diario Oficial de la Comunidades Europeas o en los correspondientes Diarios Oficiales españoles. Además se tendrán en cuenta los criterios de evaluación de la seguridad de tecnologías de información ISO 15408 (Common Criteria), en el diseño, desarrollo, evaluación y adquisición de productos y sistemas de las Tecnologías de la Información, que vayan a formar parte del *Prestador de Servicios de Certificación*, así como la normativa EESSI.

146. Los procesos de gestión de la seguridad de la infraestructura serán evaluados periódicamente.

9.3.6. Controles de seguridad de la red

147. Los medios de comunicación mediante redes públicas, que la FNMT-RCM utiliza en el desarrollo de sus actividades, utilizan suficientes mecanismos de seguridad, para evitar o controlar adecuadamente cualquier agresión externa a través de estas redes. Este sistema es auditado periódicamente con el fin de verificar su buen funcionamiento.

148. Del mismo modo, la infraestructura de la red que presta los servicios de certificación está dotada de los mecanismos de seguridad necesarios conocidos a la fecha para garantizar un servicio fiable e íntegro. Esta red también es auditada periódicamente.

9.3.7. Controles de ingeniería del módulo criptográfico

149. Entre los componentes técnicos suministrados a sus usuarios, y con objeto de incrementar la confianza de la opinión pública en sus métodos criptográficos, la FNMT-RCM realiza evaluaciones de la seguridad de los productos y servicios que ofrece, utilizando para ello criterios abiertos y aceptados por el mercado.

9.3.8. Niveles de seguridad

150. Los niveles de seguridad que tienen los distintos componentes de la infraestructura, así como los procedimientos y componentes que integran la actividad del *Prestador de Servicios de Certificación*, serán evaluados según "Criterios de Evaluación de la Seguridad de los Productos y Sistemas de las Tecnologías de la Información" (ITSEC/ITSEM) y/o Criterios Comunes (ISO15408) y, en particular, según la iniciativa EESSI.

151. Asimismo, respecto de la gestión de la seguridad de la información, ésta se realiza conforme a directrices indicadas en UNE-ISO/IEC 27001 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos".

152. Respecto de los datos personales se estará a lo especificado la normativa legal vigente y en concreto a lo dispuesto por la *LOPD* y por el Real Decreto 1720/2007, de 21 de Diciembre de desarrollo de la Ley Orgánica de Protección de Datos.

9.3.9. Procesos de auditoría y monitorización del sistema

153. La FNMT-RCM dispone de un sistema de monitorización y registro de eventos independiente de su infraestructura productiva. Este sistema funciona sin interrupción (24x7), recolectando en todo momento información y eventos de seguridad de todos los elementos sensibles y de confianza de la Autoridad de Certificación para su posterior procesamiento y correlación.

154. De este sistema de monitorización se extraen los correspondientes informes para la supervisión de la seguridad de la infraestructura. Así mismo, se dispone de reglas y políticas que proporcionan alarmas en tiempo real en caso de que existan comportamientos anómalos en los sistemas de la Autoridad de Certificación o indicios de un incidente de seguridad.

9.3.10. Restablecimiento de los servicios en caso de fallo o desastre

155. El *Prestador de Servicios de Certificación* pondrá en marcha un Plan de Recuperación ante Desastres, que contemple:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.

- Compromiso de los Datos de creación de Firma del Prestador de Servicios de Certificación. En este caso la FNMT-RCM informará a todos los miembros de la Comunidad Electrónica indicando que todos los Certificados, Listas de Revocación, Sellos de Tiempo y cualquier otra estructura de datos susceptible de firma ya no es válida debido al mencionado compromiso. La FNMT-RCM procederá al restablecimiento del servicio tan pronto como sea posible y en las nuevas condiciones aplicables.

156. La FNMT-RCM no será responsable de la falta de servicio o anomalías en el mismo, así como de los daños y perjuicios que pudieran producirse directa o indirectamente, cuando el fallo o desastre tuviera su origen en causas de fuerza mayor, atentado terrorista, sabotajes o huelgas salvajes; todo ello, sin perjuicio de realizar las actuaciones necesarias para la subsanación y/o reanudación del servicio lo antes posible.

9.3.11. Actualización de algoritmia

157. La FNMT-RCM está permanentemente informada sobre la evolución de los algoritmos criptográficos, y se compromete a actualizar el tamaño de claves o los algoritmos criptográficos utilizados por sus Autoridades de Certificación antes de alcanzar un grado de seguridad insuficiente.

9.3.12. Terminación de la actividad de la FNMT-RCM como Prestador de Servicios de Certificación

158. Esta contingencia y sus consecuencias se describen en esta *Declaración General de Prácticas de Certificación* en el apartado *"*Cese de la actividad del *Prestador de Servicios de Certificación".*

9.3.13. Control de la capacidad de prestación de los servicios

159. La FNMT-RCM realiza controles periódicos del grado de demanda de los servicios relacionados con su actividad como *Prestador de Servicios de Certificación* y de la capacidad de su infraestructura para proveer dichos servicios, como por ejemplo el sistema de información de consumos, grado de disponibilidad y ocupación de los recursos. Estos controles permiten identificar futuras inversiones en infraestructura para mantener la capacidad de prestación de los servicios.

9.4. AUDITORÍAS

160. La FNMT-RCM mantendrá un sistema específico con el fin de realizar un registro de eventos para todas aquellas operaciones como: la emisión, validación y revocación de los *Certificados*, emisión de *Listas de Revocación*, información sobre el estado de los *Certificados* y emisión de *Sellos de Tiempo*.

161. Con el objetivo de minimizar el impacto sobre los sistemas en producción, las auditorías sobre los sistemas en producción afectados se planifican en las franjas horarias de baja actividad.

9.4.1. Protección de las herramientas de auditoría

162. Todas las herramientas, informes, registros, ficheros y fuentes relacionados con la elaboración o registro de una auditoría, son considerados como información sensible y, como tal, son tratados en todos los aspectos, estando su acceso restringido a personas autorizadas.

9.4.2. Identidad del auditor

163. El auditor que verifique y compruebe la correcta operativa del *Prestador de Servicios de Certificación* de la FNMT-RCM, deberá ser una persona o profesional con la suficiente titulación oficial y la adecuada experiencia sobre la materia a auditar de acuerdo con la legislación que se encuentre en vigor en cada momento.

164. La realización de estas auditorías podrá ser encargada a Empresas Auditoras externas, a personal interno cualificado para ello (según la legislación vigente al respecto), o ambas cosas. En el caso del personal interno y dependiendo del grado de criticidad del área a auditar, el grado de independencia del personal implicado y su nivel de experiencia será objeto de concreción caso a caso, atendiendo a parámetros de independencia funcional.

165. En los casos en los que las auditorías se elaboran por personal externo a la FNMT-RCM, se establecen las medidas y controles necesarios para regular los requisitos de auditoría, el alcance, el acceso a información sensible y demás acuerdos de *Confidencialidad* y responsabilidad sobre los activos.

166. En las auditorías externas, el auditor y la empresa auditora no tendrán nunca ningún tipo de vinculación laboral, comercial o de cualquier otra índole con la FNMT-RCM, ni con la parte que solicite la auditoría, siendo siempre un profesional independiente quien realiza la auditoría solicitada.

167. Junto con el informe obtenido de la auditoría, figurará la identificación de los auditores. El informe resultado de la auditoría estará firmado por los auditores y por el responsable del ente auditado.

9.4.3. Resultados de la auditoría y acciones correctivas

168. Todas las disconformidades detectadas en la auditoría serán tratadas con las correspondientes acciones correctivas. El plan de acción de puesta en marcha de las acciones correctivas será elaborado en el plazo más breve posible y será conservado junto con el informe de la auditoría para su inspección y seguimiento en posteriores auditorías.

169. En el caso de que la deficiencia encontrada supusiera un grave riesgo para la seguridad del Sistema, de los *Certificados* o *Listas de Revocación*, de los *Datos de creación o verificación de Firma*, o de cualquier documento o dato considerado *Confidencial* en este documento, bien de los *Suscriptores*, o del propio *Prestador de Servicios de Certificación*, la FNMT-RCM actuará según lo descrito en el *Plan de Contingencias*, con el fin de salvaguardar la seguridad de toda la infraestructura.

170. De igual manera la FNMT-RCM actuará diligentemente para subsanar el error o defecto detectado en el menor espacio de tiempo posible.

9.4.4. Comunicación de los resultados

171. Las Autoridades Administrativas o Judiciales competentes podrán solicitar los informes de auditorías para verificar el buen funcionamiento del *Prestadores de Servicios de Certificación*.

9.4.5. Plan de auditorías

172. 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.
- Todas las Autoridades de Certificación incluidas en las cadenas de certificación definidas en la presente Declaración General de Prácticas de Certificación están sujetas a auditorías periódicas, según dicta el esquema de certificación correspondiente, relacionadas con
  - la iniciativa EESSI para los Prestadores de Servicios de Certificación: ETSI TS 101 456: Requisitos para las Políticas de Certificación de las Autoridades de Certificación que emiten *Certificados Cualificados*. Auditoría realizada anualmente por una empresa externa acreditada.
  - WebTrust for CA y WebTrust SSL Baseline Requirements, que aseguran que los documentos de Declaración de Prácticas y Politicas de Certificación tienen el formato y alcance adecuados, y alineados con los requisitos WebTrust mencionados. Auditoría 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 Certificación 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)

173. Se realizarán los siguientes controles:

- Controles internos de seguridad de red.
- Controles y pruebas internas del plan de contingencia.

- Controles internos de Calidad y Seguridad.
- Extraordinarios: Cuando así lo exijan las circunstancias a criterio de la FNMT-RCM.

9.4.6. Procedimiento de análisis de vulnerabilidades

174. Véase apartado "Gestión de incidentes y vulnerabilidades".

9.4.7. Procedimiento de notificación ante la detección de incidentes

175. En caso de incidente de seguridad, la notificación a las partes afectadas se realizará según lo descrito en la Política de Seguridad y su normativa de desarrollo, especialmente en el Plan de respuesta ante incidentes.

10. CONDICIONES GENERALES DE LOS SERVICIOS DE CERTIFICACIÓN

176. La FNMT-RCM está constituida como *Prestador de Servicios de Certificación* raíz, independiente, que no forma parte de estructuras de confianza externas. No obstante, dispone de la infraestructura técnica necesaria para la prestación de servicios de certificación basados en jerarquías ajenas.

177. La FNMT-RCM como *Prestador de Servicios de Certificación*, prestará servicios a todo aquel interesado que lo solicite en las condiciones previstas en esta *DGPC* y las Políticas, Prácticas y Leyes de Emisión aplicables al objeto de la solicitud.

178. Los servicios de certificación de la FNMT-RCM utilizados y combinados adecuadamente permitirán a *Usuarios*, *Suscriptores* y *Titulares*, entre otras, la dotación a los intercambios de información de las medidas de seguridad necesarias para la identificación, autenticación, no repudio y confidencialidad de las partes.

179. La FNMT-RCM gestiona sus servicios de certificación y emite certificados de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser forum y que pueden consultarse en la siguiente dirección https://cabforum.org/baseline-requirements-documents/

180. La FNMT-RCM revisará sus políticas y prácticas de certificación para mantenerlas acordes a los referidos requisitos. Ante la publicación de nuevas versiones de este documento de requisitos y en caso de encontrarse alguna inconsistencia, la FNMT-RCM actuará diligentemente para subsanar las posibles desviaciones o, en su caso, notificar en este documento los incumplimientos en los que se está incurriendo.

10.1. GESTIÓN DE LAS POLÍTICAS DE CERTIFICACIÓN

181. La FNMT-RCM dispone de *Políticas de Certificación* efectivas y específicas para cada tipo de *Certificado* o servicio de certificación. En particular, declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar las *Políticas de Certificación* a través de su Dirección General y demás órganos directivos de la misma.

- La FNMT-RCM dispone de unas *Prácticas de Certificación Particulares* en las que se detallan las prácticas de certificación aplicables a los servicios identificados en cada *Política de Certificación*.
- La FNMT-RCM dispone, dentro de las competencias de la Dirección y demás órganos directivos de la misma, 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.
- La FNMT – RCM, a través de su Comité de Gestión del Prestador de Servicios de Confianza, vela por el cumplimiento de las Declaraciones de *Políticas y Prácticas de Certificación,* las aprueba y realiza el pertinente proceso de revisión de las mismas, con una periodicidad anual.
- La FNMT-RCM realiza análisis de riesgos para evaluar las amenazas del sistema y proponer las medidas de seguridad adecuadas (salvaguardas) para todas las áreas implicadas.
- Las *Políticas y Prácticas de Certificación* se ponen a disposición del público en la dirección URL:

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

- Las *Políticas de Certificación* recogen las obligaciones y responsabilidades generales de las partes implicadas en los diferentes servicios de certificación para su uso dentro de los límites establecidos y del marco de aplicación correspondiente, siempre en el ámbito de competencias de cada una de dichas partes. Todo lo anterior se entiende sin perjuicio de las especialidades que pudieran existir en los contratos, convenios o acuerdos de aplicación.
- Para identificar cada una de las *Políticas de Certificación* se disponen de OIDs específicos. A priori no se prevé ninguna condición que implique el cambio de los OIDs identificados en esta DGPC y de las Prácticas y Políticas Particulares.
- Las *Políticas de Certificación* de la FNMT-RCM tendrán en cuenta aquella normativa y legislación de aplicación en cada caso.
- Toda la información, sistemas, procedimientos, tanto en sus aspectos cualitativos como cuantitativamente, plazos, importes, formularios y, en general, cualesquiera cuestiones manifestadas en los documentos declarativos relativos a *Políticas y/o Prácticas de Certificación*, podrán ser modificados o suprimidos por la FNMT-RCM, sin necesidad de conformidad de los miembros de la *Comunidad Electrónica* ni de las *Usuarios* de los servicios. FNMT-RCM asume el compromiso de informar de los cambios producidos a través de los sistemas establecidos en la legislación aplicable y dirección web de la entidad.
- Los miembros de la *Comunidad Electrónica* y los *Usuarios* de los servicios tienen la obligación comprobar regularmente los documentos declarativos correspondientes (*Políticas y/o Prácticas de Certificación* de aplicación), solicitando cuanta información consideren oportuna a la FNMT-RCM. No obstante, de cara a facilitar a los *Usuarios destinatarios* (*Entidad usuaria* y *Suscriptor*) el conocimiento de la existencia de novedades, cuando las modificaciones practicadas en cualquiera de las *Declaraciones*

de Prácticas de Certificación y *Políticas de Certificación* afecten directamente a los derechos y obligaciones de las partes integrantes de la *Comunidad Electrónica*, o bien restrinjan el ámbito de aplicación de los *Certificados*, la FNMT-RCM notificará a los interesados con una antelación mínima de treinta (30) días a la entrada en vigor de los cambios, con la finalidad que los miembros de la *Comunidad Electrónica* adopten la decisión que a su derecho convenga. FNMT-RCM no asumirá ningún compromiso indemnizatorio por las modificaciones o supresiones operadas en la Declaración en el ejercicio de sus derechos como *Prestador de Servicios Certificación*.

10.2. SOBRE LA GESTIÓN DE CERTIFICADOS ELECTRÓNICOS

182. Sin perjuicio de los que pudieran establecer las correspondientes las políticas, prácticas y/o Leyes de Emisión particulares de los servicios, aquellas operaciones que requieran la acreditación del interesado, ésta será realizada a través de una *Oficina de Registro*.

183. La emisión de *Certificados* supone la generación de *Documentos Electrónicos* que acrediten la identidad y, en su caso, otras cualidades o facultades del *Titular*.

184. Sin perjuicio de lo establecido en las correspondientes *Políticas y Prácticas de Certificación* particulares de los diferentes tipos de *Certificados*, la FNMT-RCM desarrollará los controles oportunos para comprobar la veracidad de la información incluida en el *Certificado*.

185. A estos efectos, cuando se trate de acreditar la identidad del *Solicitante* o *Titular* del *Certificado*, prevalecerá la personación física en la *Oficina de Registro* con el documento oficial correspondiente acreditativo de la identidad de la persona y según la legislación vigente. La FNMT-RCM tendrá en cuenta las funcionalidades previstas en la legislación aplicable en relación con el DNIe, así como otros sistemas de identificación y comprobación de las cualidades del *Titular* que aporten las garantías suficientes de la veracidad de los datos.

186. En los casos en los que en el *Certificado* se incluyan datos como nombres de dominio o direcciones IP, la FNMT – RCM comprobará, a través de los sistemas de información que los registradores autorizados para cada caso pongan a disposición del público, que la documentación exigida y validada por la *Oficina de Registro* es la correcta.

187. A tal efecto se tendrán en cuenta las publicaciones en los diferentes boletines oficinales del estado y comunidades autónomas, los registros públicos y los registros accesibles por la FNMT-RCM de las diferentes entidades registradoras de nombres de dominio y asignación de direcciones IP.

188. Todos los *Certificados*, para ser tales, y con el fin de evitar su alteración o falsificación, deberán estar firmados con los *Datos de Creación de Firma* de la FNMT-RCM en su calidad de *Prestador de Servicios de Certificación*.

189. El formato de los *Certificados* utilizados por la FNMT-RCM se basa en el definido por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, de fecha Junio de 1997 o superiores (ISO/IEC 9594-8). El formato será el especificado en la Versión 3 del mencionado formato *X.509* y será válido para el uso con protocolos de comunicación estándares tipo SSL, TLS, etc.

190. El formato de las *Listas de Revocación* publicadas por la FNMT-RCM sigue el perfil propuesto en la recomendación UIT-T X.509, en su Versión 2 en lo que se refiere a *Listas de Revocación*.

191. Para un mayor abundamiento en las prácticas y procedimientos seguidos en la emisión de de los distintos tipos de *Certificados* por parte de la FNMT-RCM se deberá consultar las *Políticas y Prácticas de Certificación* particulares y, en su caso, las *Leyes de Emisión* aplicables.

10.3. SOBRE EL SERVICIO DE INFORMACIÓN Y CONSULTA SOBRE EL ESTADO DE VALIDEZ DE LOS CERTIFICADOS

192. La información sobre el estado de los *Certificados* es proporcionada según el formato RFC 2560 – "Online Certificate Status Protocol – OCSP", entre otros.

193. La FNMT-RCM podrá prestar *Servicio de información y consulta sobre el estado de validez de los certificados* sobre *Certificados* propios o ajenos y siempre de conformidad con las políticas y prácticas particulares de aplicación y aquellos acuerdos o convenios suscritos con las terceras partes intervinientes.

10.4. SOBRE EL SERVICIO DE SELLADO DE TIEMPO

194. El formato de los *Sellos de Tiempo* emitidos por el *Servicio de Sellado de Tiempo* será según lo indicado en la RFC 3161 – "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" y la normativa ETSI 102 023 – "Requisitos para las Políticas de las Autoridades de Sellado de Tiempo"

195. Los Certificados empleados para la prestación del servicio podrán ser propios o ajenos y siempre de conformidad con las políticas y prácticas particulares de aplicación y aquellos acuerdos o convenios suscritos con las terceras partes intervinientes.

10.5. DESARROLLO DE APLICACIONES INFORMÁTICAS

196. Antes de abordar un proyecto de desarrollo de software, el *Prestador de Servicios de Certificación* sigue las pautas establecidas en la "Guía para el establecimiento de requisitos de seguridad de las aplicaciones desarrolladas en Ceres". De esta forma se garantiza que los desarrollos de las aplicaciones informáticas han sido sometidas a un proceso de valoración de riesgos y análisis de requisitos de seguridad.

197. El proceso de evolución de las aplicaciones informáticas del *Prestador de Servicios de Certificación* se realiza conforme al "Procedimiento para la gestión del cambio en las aplicaciones desarrolladas en Ceres". Dicho Procedimiento permite identificar la necesidad de realizar correcciones de emergencia o nuevas versiones de software, evaluar su impacto, incorporar los cambios aprobados y su documentación, así como verificar la consistencia de la definición del producto.

10.6. IMPARCIALIDAD DE OPERACIONES

198. La naturaleza jurídica de la FNMT-RCM, como organismo público adscrito a la Administración General del Estado, está libre de cualquier presión comercial, financiera y

de otro tipo que puedan influir negativamente en la confianza en los servicios que presta. Su estructura organizativa garantiza la imparcialidad en la toma de decisiones relativas al establecimiento, el aprovisionamiento y el mantenimiento y la suspensión de los servicios de certificación, y en particular las operaciones de generación y revocación de Certificados.

11. GESTIÓN DE INCIDENTES, VULNERABILIDADES Y CESE DE LA ACTIVIDAD

11.1. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

199. La FNMT-RCM garantiza que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información, El documento "Sistema de Gestión de la Seguridad de la Información - Manual de Seguridad" establece los procedimientos y responsabilidades para la gestión de incidentes, garantizando una respuesta rápida, efectiva y ordenada a los incidentes de seguridad.

200. En la FNMT – RCM se obtiene información sobre vulnerabilidades técnicas de los sistemas de información y se toman las medidas apropiadas. Se definen y establecen las responsabilidades asociadas con la gestión de vulnerabilidades técnicas, manteniendo los recursos de la información actualizados en el inventario de activos, para identificar vulnerabilidades técnicas. Adicionalmente, se realizan auditorías periódicas de los procedimientos emprendidos y se monitoriza y evalúa periódicamente la gestión de vulnerabilidades técnicas.

11.2. CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

201. En caso de terminación de la actividad del *Prestador de Servicios de Certificación*, la FNMT-RCM se regirá por lo dispuesto en la normativa vigente sobre firma electrónica.

202. En todo caso, la FNMT-RCM:

- Informará debidamente a los Suscriptores y Titulares de los Certificados, así como a los Usuarios de los servicios afectados, sobre sus intenciones de terminar su actividad como Prestador de Servicios de Certificación al menos con dos (2) meses de antelación al cese de esta actividad.
- Terminará cualquier subcontratación que tenga al objeto de la prestación de funciones en nombre de la FNMT-RCM del servicio a cesar
- Transferirá, con el consentimiento expreso de los Suscriptores, aquellos Certificados que sigan siendo válidos en la fecha efectiva de cese de actividad a otro Prestador de Servicios de Certificación que los asuma. De no ser posible esta transferencia los Certificados se extinguirán.
- Sea cual fuere el servicio en cese, la FNMT-RCM transferirá a un tercero los registros de eventos y auditoría, así como los Certificados y claves empleadas en la prestación del servicio, por un periodo suficiente a los efectos que dictamine la legislación vigente.

- Comunicará al Ministerio que en ese momento tenga las competencias en la materia, el cese de su actividad y el destino que vaya a dar a los Certificados, especificando en su caso: si los va a transferir, a quién, o si los dejará sin efecto. La notificación a dicho organismo se realizará con al menos dos (2) meses de antelación, en documento firmado manuscrita o electrónicamente. Además se remitirá a dicho organismo la información relativa a los Certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos pertinentes.

203. En el caso de que el cese está relacionado con el *Servicio de Sellado de Tiempo*, la FNMT-RCM:

- Tramitará la revocación de los *Certificados* de las *Unidades de Sellado de Tiempo* afectadas.
- Destruirá las C*laves privadas* de las *Unidades de Sellado de Tiempo* y sus copias de seguridad, de forma que no puedan recuperarse.

11.3. PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LOS DATOS DE CREACIÓN DE FIRMA

204. Esta contingencia está contemplada en el Plan de continuidad de negocio de la FNMT – RCM, así como el procedimiento a seguir, descrito en el Plan de gestión de la crisis como parte integrante del citado Plan de continuidad, y que determina, entre otras, las siguientes acciones a tomar:

1) Detener la prestación del servicio afectado.
2) Revocar los certificados que pudieran verse afectados.
3) Ejecutar el Plan de Comunicación con la consideración de comunicar los hechos a las partes afectadas.
4) Estudiar la necesidad de ejecutar el Cese de Actividades del PSC según la DPC y legislación vigente.

11.4. CAMBIO DE LOS DATOS DE CREACIÓN DE FIRMA DE LA FNMT-RCM

205. Esta contingencia y sus consecuencias, se describen en el apartado "Gestión del ciclo de vida de las *Claves* del *Prestador de Servicios de Certificación*" de esta *Declaración General de Prácticas de Certificación*.

12. PERFIL DE LOS CERTIFICADOS

206. Todos los *Certificados* emitidos por la FNMT – RCM son de conformidad con el estándar X.509 versión 3, salvo que las *Políticas de Certificación* y *Prácticas de Certificación Particulares* expresen lo contrario para los *Certificados* que les sean de aplicación.

12.1. RESTRICCIONES DE LOS NOMBRES

207. El nombre distintivo (*DN*) asignado al *Suscriptor* del *Certificado* dentro del dominio del *Prestador de Servicios de Certificación* será único y con la composición definida en las *Políticas de Certificación* y *Prácticas de Certificación Particulares* que le son de aplicación a cada tipo de *Certificado*.

208. La codificación de los *Certificados* sigue el estándar RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Reocation 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.

12.2. USO DE LA EXTENSIÓN POLICY CONSTRAINS

209. La extensión Policy Constrains del certificado raíz de la AC no es utilizado.

12.3. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

210. La extensión Certificate Policies incluye, como regla general y salvo que las *Políticas de Certificación* y *Prácticas de Certificación Particulares* expresen información diferente, dos campos de Policy Qualifiers:

- CPS Pointer: contiene la URL donde se publica la *Declaración General de Prácticas de Certificación* y las *Políticas de Certificación* y *Prácticas de Certificación Particulares* aplicables a los *Certificados.*
- User notice: contiene un texto que puede ser desplegado en la pantalla del usuario del *Certificado* durante la verificación del mismo.

12.4. TRATAMIENTO SEMÁNTICO DE LA EXTENSIÓN "CERTIFICATE POLICY"

211. 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.

13. TARIFAS

212. FNMT-RCM aplicará a las Administraciones Públicas las tarifas aprobadas por la Subsecretaría de la cual depende para la prestación de los servicios de certificación o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizado para tal efecto.

213. Las tarifas a aplicar al sector privado se rigen por el contrato suscrito para la provisión de los servicios de certificación. Adicionalmente, la FNMT – RCM podrá establecer las tarifas y los medios de pago que considere oportunos en cada momento. El precio y condiciones de pago podrán ser consultados en la página web de la FNMT – RCM o bien serán facilitados por el área comercial correspondiente bajo petición a la dirección de correo electrónico comercial.ceres@fnmt.es.

14. RESPONSABILIDADES FINANCIERAS

214. FNMT-RCM, como Prestador de Servicios de Certificación, está exenta de la constitución de la garantía exigida por la legislación vigente (art. 20.2. de la Ley 59/2003, de 19 de diciembre, de firma electrónica) en cuanto a un seguro de responsabilidad civil, de

conformidad con la Disposición adicional quinta de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que modificó el apartado doce del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (norma con rango de Ley que faculta a la FNMT para la prestación de servicios de intermediación y firma electrónica) , con la siguiente redacción: *«Doce. En el ejercicio de las funciones que le atribuye el presente artículo, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda estará exenta de la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la Ley 59/2003, de Firma Electrónica».*

215. No obstante lo anterior, la FNMT-RCM, además de ser un organismo público del Estado Español, cuenta con un seguro de responsabilidad civil específico para la actividad como Prestador de Servicios de Certificación, con un límite de cobertura de 4.500.000,00 Euros.

15. DATOS DE CARÁCTER PERSONAL

216. El régimen de protección de datos de carácter personal derivado de la aplicación de la presente *Declaración General de Prácticas de Certificación* y en su caso de la actuación conjunta con cualquier Administración, será el previsto en la Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en su normativa de desarrollo. Los ficheros serán de titularidad pública y su creación, modificación o supresión se realizará por disposición general publicada en el Boletín Oficial del Estado.

217. Como consecuencia de la prestación de servicios EIT, las *Oficinas de Registro* podrán acceder al fichero de usuarios de Sistemas Electrónicos, Informáticos y Telemáticos. En cualquier caso, será la FNMT-RCM en su condición de *Responsable del Fichero* la que decida sobre la finalidad, contenido y uso del tratamiento de los datos, limitándose las *Oficinas de Registro*, como *Encargadas del Tratamiento*, a utilizar los datos de carácter personal contenidos en dicho fichero, única y exclusivamente para los fines que figuran en su *Declaración General de Prácticas de Certificación*. La *Oficina de Registro* en cumplimiento con lo establecido en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal se compromete a:

- Tratar los datos siguiendo estrictamente las instrucciones de la FNMT-RCM.
- No aplicar o utilizar los datos personales obtenidos, para fines distintos a los que figuren en la presente Declaración General de Prácticas de Certificación.
- No comunicarlos a terceros, ni siquiera para su conservación.
- Guardar secreto profesional respecto de los mismos, aun después de finalizar sus relaciones con la FNMT-RCM y trasladar las obligaciones citadas en los párrafos anteriores al personal que dediquen al cumplimiento de la presente Declaración General de Prácticas de Certificación.
- Adoptar las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, de conformidad con lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

- Destruir o devolver todos los datos de carácter personal objeto de tratamiento una vez finalice por cualquier causa la relación con la FNMT-RCM, salvo aquellos datos que la legislación obliga a conservar por un mínimo de quince (15) años.

218. Sin perjuicio de otras obligaciones, la *Oficina de Registro* verificará que el *Suscriptor* y el *Titular* son informados y prestan su *Consentimiento* para el tratamiento de sus datos, con las finalidades y comunicaciones previstas en los documentos de *Consentimiento* correspondiente. Asimismo comprobará que se han cumplimentado correctamente todos los campos de datos personales necesarios para la prestación del servicio.

219. Las *Oficinas de Registro* informarán de esta obligación a todo su personal y responderán de cualquier perjuicio que se le produzca a la FNMT-RCM como consecuencia del incumplimiento de estas obligaciones en la recogida de datos, debiendo asimismo y en este sentido, mantenerla a salvo de reclamaciones de terceros o de sanciones administrativas.

220. Los datos personales del *Solicitante* una vez validados y, en su caso, su código de solicitud, recogidos en la fase de solicitud del *Certificado*, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

221. La FNMT-RCM no admitirá como *Suscriptor* o *Titular* del *Certificado*, alias, seudónimos o nombres interpuestos distintos de la identidad personal del *Suscriptor* o *Titular* que se recoge en el Documento Nacional de Identidad, o Documento de Identificación de Extranjeros.

222. La FNMT-RCM podrá identificar, cuando así se requiera, a los *Usuarios* de los servicios de certificación a través de otros *Certificados*. En estos casos y en los que se refiere a la protección de datos de carácter personal de los *Usuarios* de los servicios será de aplicación, además de las normas antes citadas, lo declarado para la gestión de *Certificados*.

15.1. INFORMACIÓN AL SUSCRIPTOR

223. De conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa al *Suscriptor* y *Titular* que los datos de carácter personal que se incluyan en los formularios o contratos que se le presenten durante su personación a la hora de solicitar la emisión de un *Certificado* se registrarán en el fichero de usuarios de Sistemas Electrónicos, Informáticos y Telemáticos (EIT), establecido por la Orden EHA/2357/2008, de 30 de julio (BOE de 7 de agosto), por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM, y del que será responsable la FNMT-RCM.

224. La prestación de los servicios EIT solamente podrá realizarse si se cumplimenta y responde en su totalidad y con datos e información verdadera a los formularios. Dichos datos son recogidos con la finalidad de prestar los servicios de certificación en los términos establecidos en la normativa vigente y en la presente *Declaración General de Prácticas de Certificación*. Mediante su compleción, las partes consienten el tratamiento de sus datos para los usos y finalidades previstas, sin perjuicio del ejercicio de los derechos reconocidos a estos efectos en la legislación aplicable.

225. Los datos de carácter personal podrán ser comunicados sin consentimiento de los *Titulares* o *Suscriptores* del *Certificado* a otras Administraciones Públicas, sus organismos autónomos

y demás entidades vinculadas o dependientes con el objetivo que éstas ejerzan sus respectivas competencias y siempre dentro del ámbito del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, y normativa de desarrollo. Todo ello, a los efectos de garantizar la prestación de los servicios de certificación y con la finalidad de comprobar la vigencia de los *Certificados* emitidos a los *Titulares,* permitiendo así la realización a través de medios electrónicos, informáticos y telemáticos de actuaciones en el ámbito de relaciones de derecho público.

226. Asimismo, los datos de carácter personal podrán ser cedidos y/o comunicados a los miembros de la *Comunidad Electrónica* que no tengan la consideración de Administración pública y/o Organismos públicos, de acuerdo con el artículo 11.2.c de la LOPD en el ámbito de relaciones de derecho privado, cuando sea necesaria la cesión y/o comunicación para el desarrollo, cumplimiento y control de los servicios contratados y/o solicitados a la FNMT-RCM por los *Titulares* y *Suscriptores* de los certificados o personas o entidades autorizadas por estos titulares del certificado. Esta cesión y/o comunicación se realizará exclusivamente para cumplir con el fin propio para el que ha sido emitido el *Certificado,* de acuerdo con la normativa sobre firma electrónica y atendiendo a los usos que vaya a realizar el titular del certificado en los términos del contrato y/o acuerdos correspondientes con la FNMT-RCM y terceros autorizados.

227. El titular de los datos podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, cuando la FNMT-RCM sea el responsable del fichero dirigiéndose para ello a la Secretaría General de la FNMT-RCM sita en la calle Jorge Juan, número 106, 28071 de Madrid o bien a través de

https://www.sede.fnmt.gob.es/certificados/persona-fisica/modificar-datos

(modificación de datos personales), sin perjuicio de la obligaciones de conservación que establezca la Ley. Asimismo, para conocer el ámbito de la *Comunidad Electrónica* podrá verificar su composición a los efectos señalados en la misma dirección web ejerciendo los derechos que correspondan.

228. La FNMT-RCM adopta los niveles de seguridad requeridos por el Reglamento de Medidas de Seguridad aprobado por el Real Decreto 1720/2007 de 21 de diciembre.

15.2. INFORMACIÓN A LA ENTIDAD USUARIA

229. Los datos contenidos en el *Directorio* seguro de *Certificados* tienen la consideración de datos de carácter personal a efectos de lo dispuesto en la *LOPD* y demás normativa complementaria, y por este motivo, la FNMT-RCM no permite que sean accedidos.

230. Sin embargo, la FNMT-RCM sí pone a disposición de las personas y *Entidades usuarias* las listas de certificados revocados (que no contiene datos personales) para el cumplimiento diligente de los servicios de certificación de acuerdo con la Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM. Las *Entidades usuarias* como cesionario de esta información únicamente podrá utilizarla de acuerdo con esas finalidades.

231. No obstante, y con carácter general, cualquier registro o utilización para otros fines distintos de los anteriores o no autorizados requiere del *Consentimiento* previo de los titulares de los datos así como de otras previsiones contempladas en la Ley. Su incumplimiento está

sancionado en la *LOPD* con multas que pueden alcanzar los 600.000 euros por cada una de las infracciones cometidas y sin perjuicio de la incoación de acciones penales de acuerdo con el Capítulo I del Título X del Código Penal así como de reclamaciones privadas de los afectados.

232. La FNMT-RCM de conformidad con la legislación reguladora del DNIe podrá realizar servicio de validación sobre la vigencia de los certificados electrónicos incorporados en el DNIe, por lo que en los supuestos que sea factible la identificación electrónica con el DNIe para acceder a servicios previstos en la presente DGPC, FNMT-RCM estará autorizada por los sujetos titulares del DNIe con la funcionalidad informática activada, para la cesión y/o comunicación a otros miembros de la *Comunidad Electrónica* cuando sea necesario en el ámbito de relaciones de derecho público y/o privado a los efectos previstos en el art. 11.2 c) de la LOPD.

15.3. DOCUMENTO DE SEGURIDAD LOPD

15.3.1. Objetivo y presentación del Documento de Seguridad LOPD

233. El objetivo de este documento es establecer las medidas de seguridad a implantar por la FNMT-RCM en el entorno del *Prestador de Servicios de Certificación*, para la protección de los datos de carácter personal, contenidos en el Fichero de Usuarios de Sistemas Electrónicos, Informáticos y Telemáticos (EIT), registrado en la *AEPD* e identificados en la Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM.

234. La FNMT-RCM como *Prestador de Servicios de Certificación*, precisa disponer de datos de carácter personal de sus usuarios registrados, con el fin de poder identificarlos y proporcionar los *Datos de verificación de Firma* y prestar los servicios de certificación correspondientes, indispensables para relacionarse a través de medios electrónicos, informáticos y telemáticos. Dada la naturaleza de este tipo de datos, según indica el Real Decreto 1720/2007 de 21 de diciembre, se deben adoptar medidas de seguridad de nivel medio.

235. La presente Normativa de Seguridad tiene por objeto preservar los datos personales procesados dentro del *Prestador de Servicios de Certificación* de la FNMT-RCM, por lo que afectará a todos aquellos recursos (personal, máquinas, aplicativos, métodos) que estén implicados en el procesamiento de estos datos. Desde el Sistema de Información que desempeña las funciones de registro de los usuarios, donde se recaban los datos, hasta el almacenamiento y archivo de los mismos en sistemas de *Directorio Seguro*, sistemas identificación y/o autorización, sistemas de archivado y registro de eventos y cualquier otro que pudiera existir interviniente en la prestación de servicios de certificación, incluyendo los interfaces y medios de comunicación entre los diferentes sistemas, ya sean redes telemáticas privadas o públicas.

236. Este documento es de obligado cumplimiento para todo el personal perteneciente al *Prestador de Servicios de Certificación* de la FNMT-RCM, así como para todas las personas relacionadas con la misma, que requieran acceso a los datos de carácter personal.

237. La responsabilidad de todos los ficheros que contienen datos de carácter personal declarados por la FNMT-RCM corresponde a dicha entidad, ya que es la persona jurídica que decide

sobre la finalidad, usos y contenido de los ficheros. No obstante, en lo que respecta al Fichero de "Usuarios de Sistemas EIT", el Director de Sistemas de Información de la FNMT-RCM es la persona facultada para decidir y autorizar sobre el uso y tratamiento de éste en representación de la FNMT-RCM.

238. Dentro del ámbito se incluyen las *Oficinas de Registro* como entidades colaboradoras de la FNMT-RCM como *Prestador de Servicios de Certificación*, que tienen la misión de llevar a cabo la identificación y autenticación del ciudadano, registrando sus datos personales con destino al *Prestador de Servicios de Certificación* de la FNMT-RCM.

15.3.2. Normas y estándares

239. Las leyes, normas y estándares que han sido considerados para la elaboración de este documento, sin perjuicio de las actualizaciones que puedan producirse, son:

Directivas Europeas

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Legislación Española

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1736/1998, de 31 de julio, que desarrolla el Título III de la Ley General de Telecomunicaciones (Reglamento de Servicio Público).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999
- Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM

15.3.3. Principios y normas de obligado cumplimiento

240. Este apartado recoge todos aquellos aspectos necesarios de obligado cumplimiento que dan respuesta a los apartados establecidos en el *artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999 (RD 1720/2007).*

Funciones y obligaciones del personal

241. Este Documento así como cualquier nueva versión del mismo y aquellos que representan las políticas y prácticas particulares de los diferentes servicios de certificación, son conocidos por todas las personas pertenecientes al *Prestador de Servicios de Certificación* de la FNMT-RCM o que tienen obligación de tratar con dichos datos de carácter personal.

242. Existen una serie de funciones claramente diferenciadas en lo que respecta al personal implicado en el uso y tratamiento de los datos de carácter personal del Fichero de Usuarios

de Sistemas EIT, como son: El *Responsable del Fichero*, el *Responsable de Seguridad*, el *Personal de Seguridad Informática*, *Administrador de la Aplicación*, *Usuarios de la Aplicación*, *Operador de backup*, *Auditor de Seguridad*. Estas funciones y, en su caso las personas que las asumen, se definen en el punto "*Documento de Seguridad LOPD*" del apartado "Definiciones" de la presente *Declaración General de Prácticas de Certificación*.

Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan

243. La estructura de los ficheros de carácter personal utilizados por el *Prestador de Servicios de Certificación* de la FNMT-RCM, es la que se recoge en el Fichero de Usuarios de Sistemas EIT, que ha sido declarado a la *Agencia Española de Protección de Datos* y que viene descrita en el ANEXO de la Orden EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM, estando el fichero identificado como "Fichero de usuarios de sistemas electrónicos, informáticos y telemáticos (EIT)"

244. Los subsistemas que tienen algún tipo de implicación en el tratamiento de los datos de carácter personal en el ámbito del Real Decreto 1720/2007, se relacionan y describen de forma resumida a continuación:

Subsistema de Gestión de Certificados

245. Cuya misión es la creación de los *Certificados* de acuerdo al estándar *X.509*, donde se introducen las *Claves* creadas por el subsistema de generación de *Claves* y otros datos identificativos.

Subsistema de Oficina de Registro

246. Tiene como objetivo la identificación y autenticación del *Suscriptor*, donde son registrados sus datos personales para proceder a su envío, de forma cifrada, al *Prestador de Servicios de Certificación* de la FNMT-RCM.

Subsistema de Publicación

247. Tiene como misión la gestión de la publicación del *Directorio* del *Prestador de Servicios de Certificación* de la FNMT-RCM y las *Listas de Revocación.*

Procedimiento de notificación, gestión y respuesta ante las incidencias

248. Los datos de carácter personal subyacen en *Certificados*, estructurados de acuerdo al estándar *X.509*, siendo algunos de estos datos de uso público.

249. El procedimiento de acceso, rectificación, cancelación y oposición de los datos de carácter personal está formalizado. Puede ser ejercido en la Secretaría General de la FNMT-RCM o en la página web del *Prestador de Servicios de Certificación* de la FNMT-RCM.

250. Las incidencias de destrucción accidental de información de los datos de carácter personal se solucionan con copias de seguridad dotadas de *Disponibilidad*, almacenadas y gestionadas de forma adecuada y debidamente protocolizada.

251. Existe una base de datos de incidencias en la que se abren y se gestionan las incidencias. Cada persona puede realizar diferentes gestiones en función del rol que desempeñen. De modo resumido, cualquier persona perteneciente al PSC puede abrir una incidencia. Éstas son tratadas por personal del área correspondiente y una vez resuelta se cierra con la

descripción de las acciones realizadas. En caso de que la incidencia conlleve modificaciones se abre una acción correctiva que es ejecutada por el personal al que compete la acción.

252. Los principales campos de una incidencia son:

- Nombre de la incidencia (breve descripción)
- Persona que abre la incidencia, fecha de apertura
- Área a la que, en principio, compete la incidencia
- Prioridad
- Tipo (en general se corresponde con el Hardware/Software afectado)
- Descripción (descripción detallada de la incidencia)
- Acciones (acciones realizadas para solucionar la incidencia
- Registro de personas que manejan la incidencia.

Procedimientos de copias de seguridad y recuperación de datos

253. En la Política de backup / recuperación del *Prestador de Servicios de Certificación* se han definido seis tipos diferentes de datos, atendiendo a sus requerimientos de copia y respaldo. Todos los datos tratados por la *Infraestructura de Clave Pública* han sido clasificados en alguno de estos "Tipos".

254. Los Tipos que se refieren a datos personales son los siguientes:

TIPO 3. Información de auditoría: Muestran el funcionamiento de los sistemas y entornos de aplicación a lo largo del tiempo, y constituyen evidencias y rastros de las acciones que se están realizando y las aplicaciones que se ejecutan. Por lo tanto puede contener información relativa a datos personales de sus clientes.

TIPO 5. Datos personales: Datos asociados a personas físicas identificadas o identificables, ya sean considerados privados o públicos.

TIPO 6. Claves: Básicamente, se engloban en esta categoría las claves maestras de acceso a los sistemas y entornos de aplicación, claves críticas de los sistemas, claves de administración y usuarios de emergencia. Su uso es ocasional.

255. Las características que se han definido para la realización de copias de seguridad, tienen en cuenta los siguientes factores:

- Periodicidad de la copia de seguridad (frecuencia con la que deben realizarse)
- Duración de las copias de seguridad (tiempo que deberán mantenerse las copias)
- Tipo de copia de seguridad (total o incremental)
- Almacenamiento (destino de las copias de seguridad)
- Cifrado (dota de Confidencialidad)
- Firmado (dota de Integridad y autenticidad)

256. Concretamente para los datos de Tipo 5, es decir, datos de carácter personal, se han definido las siguientes características:

- Periodicidad de la copia de seguridad: Se realizará como mínimo, una copia diaria de seguridad y respaldo de estos datos, cumpliendo lo exigido por la legislación aplicable.
- Duración de las copias de seguridad: Las copias de seguridad se almacenarán durante un período de siete días laborables.
- Tipo de copia de seguridad: Las copias de backup se realizarán siempre completas.
- Almacenamiento: Las copias de seguridad y respaldo se almacenarán en el archivo ignífugo de alta seguridad del *Prestador de Servicios de Certificación* de la FNMT-RCM.
- Cifrado: La información no irá cifrada
- Firmado: La información no irá firmada.

257. La información detallada sobre estas clasificaciones se encuentra en el *Manual de Seguridad* del *Prestador de Servicios de Certificación* de la FNMT-RCM. En dicho manual se definen los responsables de las copias, quiénes pueden acceder a ellas y a quién deben comunicárselo en caso de incidencia.

258. Mayor nivel de detalle sobre este proceso se encuentra descrito en el documento sobre la política de copias seguridad, respaldo y recuperación de la infraestructura denominado "Política de backup / recuperación".

Control de acceso

259. Sólo se tiene acceso a los datos de acuerdo al perfil asignado y siempre que dicho acceso sea necesario para el desempeño de las distintas funciones.

260. Por ejemplo, la *Oficina de Registro* debe proporcionar los requerimientos de control de acceso al sistema de información del *Prestador de Servicios de Certificación* de la FNMT-RCM a los registradores, proporcionándoles el nivel de acceso para llevar a cabo la función de registro.

- Control de acceso basado en perfiles: usando la identidad o el perfil del usuario del sistema, que solicita un acceso, junto con el modo de acceso solicitado.
- Se permitirá el acceso siempre que el usuario identificado solicite un modo de acceso que haya sido autorizado previamente; de lo contrario, se denegará.

261. El *Responsable del Fichero* ha establecido mecanismos para evitar que un usuario pueda acceder a datos de carácter personal con derechos distintos al permitido y para impedir el intento reiterado de acceso no autorizado al sistema de información.

Régimen de trabajo fuera de los locales de la ubicación del fichero

262. Todos los trabajos sobre los datos personales se llevan a cabo en el centro de trabajo de la FNMT-RCM como *Prestador de Servicios de Certificación*.

263. Tal como se ha comentado en el apartado anterior la función de registro se lleva a cabo en las *Oficinas de Registro* por personas debidamente autorizadas.

Ficheros temporales

264. El software disponible para el tratamiento de datos de carácter de personal necesarios para crear un certificado electrónico de acuerdo al estándar *X.509* genera ficheros temporales (ficheros de logs) que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

265. En cualquier caso, estos ficheros tienen el mismo nivel de seguridad que el fichero declarado y por tanto se les aplica los mismos controles de seguridad.

Gestión de soportes

266. Los soportes informáticos que contienen datos de carácter personal están diligentemente identificados, pudiéndose identificar el tipo de información que contienen. Asimismo son almacenados en un lugar de acceso restringido al personal autorizado y custodiado por el personal de seguridad.

267. En el caso de que se produjese una salida de un soporte informático que contenga datos de carácter personal fuera del centro de trabajo del *Prestador de Servicios de Certificación* de la FNMT-RCM, únicamente podrá ser autorizada por el *Responsable del Fichero*.

268. La destrucción de soportes se realiza previa baja de dicho soporte de la "aplicación de backup" (aplicación de copia de seguridad y respaldo que actúa como inventario de soportes) y consiste en la destrucción física del soporte (extracción de la cinta magnética de su contenedor y triturado de la misma).

269. Existe un sistema de registro de entrada de soportes, que permite directa o indirectamente conocer:

- El tipo de soporte.
- La fecha y hora de entrada.
- El emisor.
- El número de soportes.
- El tipo de información que contiene.
- La forma de envío.
- La persona responsable de recibir la información, que en todo caso está debidamente autorizada por el Responsable del Fichero

270. Asimismo, existe un sistema de registro de salida de soportes que permite directa o indirectamente conocer:

- El tipo de soporte.
- La fecha y hora de salida.
- El destinatario.
- El número de soportes.
- El tipo de información que contiene.
- La forma de envío.

- La persona responsable de la entrega, que en todo caso está debidamente autorizada por *el Responsable del Fichero*

271. Cuando un soporte vaya a ser desechado o reutilizado se seguirá el procedimiento previsto para impedir cualquier recuperación posterior de la información almacenada en él. Este procedimiento se seguirá previamente a que se proceda a la baja del soporte en el Inventario.

272. Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Auditoría

273. Para el cumplimiento de todos los aspectos señalado en la *LOPD* se llevará a cabo una auditoría que verifique el cumplimiento de las normas e instrucciones indicadas en este documento. Esta auditoría se llevará a cabo al menos una vez cada dos (2) años.

274. Este informe de auditoría hace referencia a la adecuación de las normas e instrucciones indicadas en este documento, identificando las debilidades y proponiendo las acciones correctoras pertinentes. Asimismo, en el informe se incluyen los datos, hechos y observaciones en que se base el informe realizado, así como las recomendaciones propuestas.

Acceso Lógico

275. Existen varios tipos de acceso lógico al fichero:

- Acceso con usuario y contraseñas (paswords): acceso en el que un usuario de la aplicación busca la Clave Pública de un Titular partiendo de los datos de identificación del mismo ("serial number" del Certificado, "common name", etc.).
- Acceso privilegiado al Directorio o base de datos, donde se encuentran almacenados todos los datos de carácter personal. Para realizar este tipo de acceso es necesario realizar un alta en la aplicación de acuerdo a lo dispuesto en la normativa de seguridad del Prestador de Servicios de Certificación de la FNMT-RCM.

276. Los parámetros que están configurados y que incluyen lo exigido por el Reglamento de la *LOPD* son los que a continuación se describen:

- Cada usuario se identifica ante la aplicación con un nombre de usuario, que es único para cada persona.
- Todo usuario para autenticarse debe introducir una contraseña, que únicamente debe conocer el usuario que pretende autenticarse. Cada usuario es responsable de su contraseña y no debe compartirla con ningún otro.
- No se han creado grupos de personas que puedan acceder con un mismo usuario y contraseña, y tampoco existen usuarios genéricos. Las cuentas genéricas que se creen para pruebas o similares se eliminan inmediatamente después de realizar dichas pruebas.
- Cada usuario es libre de cambiar su contraseña si cree que esta puede estar comprometida, pero para ello debe haberla utilizado al menos durante un día. Sin

perjuicio de lo anterior, el usuario tiene la obligación de no usar la misma contraseña durante un periodo superior a tres (3) años.

- Cuando un usuario se identifica y autentica más de tres veces de forma errónea el sistema bloquea la cuenta de dicho usuario.
- Existe un mecanismo de control: el Registro de Eventos, encargado de almacenar, entre otra información, todos los accesos a los distintos componentes de la infraestructura.

Acceso Físico

277. Solo el personal debidamente autorizado tiene acceso físico a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal, esto es, al CPD del *Prestador de Servicios de Certificación* de la FNMT-RCM.

278. Para acceder a estas instalaciones, se dispone de un sistema de control de acceso mediante lectores de tarjeta y teclados.

279. Periódicamente, se lleva a cabo un control de los registros de eventos generados por el Sistema de control de acceso, que permitirá detectar cualquier tipo de anomalía en la operativa diaria.

Pruebas con datos reales

280. Las pruebas en el desarrollo de las aplicaciones que tratan el Fichero EIT, no se hacen con datos reales.

281. Los distintos aplicativos que requieren acceso a dicho fichero se realizan con carga de datos de prueba.

15.3.4. Proceso de revisión

282. El apartado "Documento de Seguridad *LOPD*" ha sido confeccionado para cumplir con Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

283. El Documento se mantendrá actualizado. Todas las modificaciones que se produzcan como consecuencia de mejoras o adaptación por normativa legal se incorporarán al Documento.

16. PROPIEDAD INTELECTUAL E INDUSTRIAL

284. La FNMT-RCM es titular en exclusiva de todos los derechos, incluidos los derechos de explotación, sobre el *Directorio* seguro de *Certificados*, *Listas de Revocación*, servicios de información sobre el estado de los *Certificados* y servicios de *Sellado de Tiempo* en los términos señalados en el Texto Refundido de la Ley de Propiedad Intelectual aprobado mediante Real Decreto Legislativo 1/1996, de 12 de abril (Ley de Propiedad Intelectual), incluido el derecho *sui generis* reconocido en el artículo 133 de la citada Ley. En consecuencia, el acceso a los *Directorios* seguros de *Certificados* queda permitido a los miembros de la *Comunidad Electrónica* legitimados para ello, quedando prohibida cualquier reproducción, comunicación pública, distribución, transformación o reordenación salvo cuando esté expresamente autorizada por la FNMT-RCM o por la Ley. Queda asimismo prohibida la extracción y/o reutilización de la totalidad o de una parte sustancial del

contenido, ya sea considerada como tal desde una perspectiva cuantitativa o cualitativa, así como su realización de forma repetida o sistemática.

285. El acceso a los servicios de información sobre el estado de los *Certificados* y servicios de *Sellado de Tiempo* estará restringido según lo dispuesto en las políticas y prácticas particulares que regulen dichos servicios.

286. La FNMT-RCM mantiene todo derecho, título y participación sobre todos los derechos de propiedad intelectual e industrial y conocimiento relativos a la presente *Declaración General de Prácticas de Certificación*, los documentos declarativos (políticas y prácticas) que particularicen o completen esta DGPC, los servicios que preste, y los programas de ordenador o hardware que utilice en dicha prestación de servicios.

287. Asimismo, tanto la *Tarjeta criptográfica* utilizada como soporte para almacenar los *Certificados* y *Claves* criptográficas, como la información generada mediante la prestación de los servicios por la FNMT-RCM será en todo momento propiedad exclusiva de la FNMT-RCM.

288. Respecto de la *Tarjeta criptográfica*, la FNMT-RCM otorga únicamente un derecho de uso a los *Suscriptores* de los *Certificados*, para que la utilicen como soporte para almacenar y utilizar los *Certificados* y *Claves* criptográficas emitidos por la FNMT-RCM o por otro *Prestador de Servicios de Certificación*.

289. Los *OID* utilizados en los *Certificados* emitidos, en los *Certificados* empleados para la prestación de los servicios, en los *Sellos de Tiempo* y para el almacenamiento de ciertos objetos en el *Directorio*, son propiedad de la FNMT-RCM y han sido registrados en el IANA (Internet Assigned Number Authority) bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA-Registered Private Enterprises), habiéndose asignado el número 1.3.6.1.4.1.5734 (FABRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA). Esto puede ser consultado y comprobado en:

http://www.iana.org/assignments/enterprise-numbers

290. Queda prohibido, de no mediar un acuerdo expreso y firmado con la FNMT-RCM, el uso total o parcial de cualquiera de los *OID* asignados a la FNMT-RCM salvo para los menesteres específicos para los que se incluyeron en el *Certificado* o en el Directorio.

291. Queda prohibida la reproducción o copia incluso para uso privado de la información que pueda ser considerada como Software o Base de Datos de conformidad con la legislación vigente en materia de Propiedad intelectual, así como su comunicación pública o puesta a disposición de terceros.

292. Queda prohibida cualquier extracción y/o reutilización de la totalidad o de una parte sustancial de los contenidos o de las bases de datos que la FNMT-RCM ponga a disposición de los *Suscriptores* o *Entidades usuarias*.

16.1. PRESTACIÓN DE SERVICIOS DE VALIDACIÓN DE CERTIFICADOS PARA EL TRAMO MAYORISTA

293. Los servicios de validación de certificados realizados por la FNMT-RCM, principalmente mediante protocolo OCSP, no podrán ser objeto de reservicio, con o sin reventa, sin que exista valor añadido a los mismos. En caso de que se proporcione ese valor añadido para

terceras partes, basándose en servicios de validación prestados por la FNMT-RCM, se debe solicitar a esta entidad la suscripción de un contrato OCSP para el tramo mayorista. Tal contrato se encuentra disponible en la página Web de la FNMT-RCM (Perfil del Contratante) y el solicitante deberá cumplir los requerimientos para su calificación como mayorista (prestación de servicios para terceros).

294. La FNMT-RCM quedará exonerada de responsabilidad por actuaciones de personas, entidades u organizaciones que sin suscribir un contrato para el tramo mayorista, procedan a realizar estos servicios para terceros. Todo ello sin perjuicio de las acciones legales que pudieran corresponder.

17. ORDEN DE PRELACIÓN

295. Las distintas *Políticas y Prácticas de Certificación* Particulares tendrán prevalencia en lo que corresponda con carácter particular y referido a los tipos de *Certificados* y/o servicios que tratan, sobre lo dispuesto en el cuerpo principal de la presente *Declaración General de Prácticas de Certificación*.

18. LEY APLICABLE, INTERPRETACIÓN Y JURISDICCIÓN COMPETENTE

296. Todas las *Políticas y Declaraciones de Prácticas de Certificación* de la FNMT-RCM, se regirán por lo dispuesto por las Leyes del Reino de España.

297. Con carácter general, los miembros de la *Comunidad Electrónica* y los *Usuarios* de los servicios de certificación de la FNMT-RCM aceptan que todo litigio, discrepancia, cuestión o reclamación resultante de la ejecución o interpretación de las *Políticas y/o Declaraciones de Prácticas de Certificación* o relacionada con ellas, directa o indirectamente, se resolverá de conformidad con lo establecido en los correspondientes contratos y/o convenios, en los términos previstos en el Estatuto de la entidad, aprobado por RD 1.114/1999, de 25 de junio (BOE nº 161 de 7 de julio). Asimismo, podrán pactarse, previa aprobación de los órganos competentes de la FNMT-RCM, cláusulas de arbitraje, de acuerdo con lo establecido en la Legislación aplicable.

19. PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN Y FIRMA ELECTRÓNICA SOBRE CERTIFICADOS PROPIOS

298. FNMT-RCM, si no existiera prohibición legal, podrá realizar su actividad como prestador sobre certificados electrónicos propios cuando en el desarrollo de otros fines distintos a los servicios de certificación fuera necesario actuaciones de validación y/o otros servicios con los diferentes miembros de la *Comunidad Electrónica*.

299. En caso de conflicto de intereses, por la actividad antes señalada, entre la FNMT-RCM y otros miembros de la *Comunidad Electrónica,* ambas partes podrán someter su discrepancia a la intervención de uno o más árbitros, o dirimirla ante los juzgados o tribunales competentes según las reglas de la jurisdicción antes señaladas.

ANEXO: PERFIL DEL CERTIFICADO RAÍZ FNMT – RCM

Campo		Contenido	Ext. Crítica	Especificaciones
1. Version		2		Integer:=2 ([RFC5280] describe la versión del certificado. El valor 2 equivale a decir que el certificados es versión 3 (X509v3)
2. Serial Number		Número identificativo único del certificado.		Establecido automáticamente por la Entidad de Certificación. [RFC5280]. Será un "integer" positivo, no mayor 20 octetos (1- 2^{159}). El número de serie se asignará de forma aleatoria.
3. Signature Algorithm		Sha256withRsaEncryption		OID: 1.2.840.113549.1.1.11
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)		
	4.1. Country	C=ES		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM		UTF8 String
	4.3. Organization Unit	OU=AC RAIZ FNMT-RCM		UTF8 String
5. Validity		Hasta 01/01/2030		Formato UTCTime, de acuerdo con RFC 5280
6. Subject				
	6.1. Country	C=ES		Se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements". PrintableString, tamaño 2 (rfc5280)
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado). O=FNMT-RCM.		UTF8 String
	6.3. Organization Unit	OU=AC RAIZ FNMT-RCM		UTF8 String
7. Subject Public Key Info		Algoritmo: RSA Encryption Longitud: 4096 bits		Campo para transportar la clave pública y para identificar el algoritmo asociado.

Campo			Contenido	Ext. Crit ica	Especificaciones
8. Subject Key Identifier			Identificador de la clave pública de la CA. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.		RFC 5280: hash SHA-1 de 20 bytes calculado sobre el valor BIT STRING del campo subjectPublicKey (excluyendo etiqueta, longitud y número de bits no usados).
9. Key Usage			Uso permitido de las claves certificadas.	Sí	Normalizado en norma X509 y RFC 5280
	9.1. Digital Signature		0		Ver X509 y RFC 5280
	9.2. Content Commitment		0		Ver X509 y RFC 5280
	9.3. Key Encipherment		0		Ver X509 y RFC 5280
	9.4. Data Encipherment		0		Ver X509 y RFC 5280
	9.5. Key Agreement		0		Ver X509 y RFC 5280
	9.6. Key Certificate Signature		1		Ver X509 y RFC 5280
	9.7. CRL Signature		1		Ver X509 y RFC 5280
10. Certificate Policies			Política de certificación		
	10.1. Policy Identifier		2.5.29.32.0 (anyPolicy)		Atendiendo a la rfc5280: " *In a CA certificate,these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }*"
	11.2. Policy Qualifier Id				
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/		IA5String String. URL de las condiciones de uso.
11. Basic Constraints				Sí	
	11.1. cA		Valor TRUE (CA)		De la rfc 5280: "The cA boolean indicates whether the certified public key may be used to verify certificate signatures."
	11.2. pathLenConstraint		Ninguna		No existe restricción de longitud de ruta a nivel de CA Raíz