Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DECLARACIÓN GENERAL DE PRÁCTICAS DE SERVICIOS DE CONFIANZA Y DE CERTIFICACIÓN ELECTRÓNICA

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	28/01/2026
Revisado por:	FNMT-RCM	28/01/2026
Aprobado por:	FNMT-RCM	29/01/2026

Versión	Fecha	Descripción
		Declaración de Prácticas de Certificación (de todas las políticas de certificación de la FNMT-RCM)
3.0	05/05/2009	Creación del documento
3.1	04/01/2010	Actualización de aspectos relativos al servicio de sellado de tiempo
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.
3.3	19/12/2011	Se incluye un apartado específico sobre la gestión de *Políticas de Certificación*
3.4	20/01/2012	Se incluye una nueva redacción del párrafo 12.1 describiendo las condiciones de reventa de los servicios.
3.5	02/07/2013	Se incluye la periodicidad de un año para la realización de auditorías conforme a la norma ETSI 101-456 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.

Versión	Fecha	Descripción
		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.
4.1	16/02/2015	Inclusión del compromiso con los requisitos base definidos por el CA/Browser forum
4.2	14/07/2015	Inclusión del compromiso con los requisitos definidos por la ETSI 101 456.
4.3	12/04/2016	Incorporación de referencias a ACs Usuarios y Representación y eliminación de ACs APE y AC ISA.
5.0	24/06/2016	Cumplimiento requisitos ETSI 101456 y actualización definiciones conforme el Reglamento (UE) No 910/2014 (eIDAS).
5.1	03/01/2017	Actualización a Reglamento eIDAS (ETSI 319 401).
5.2	09/10/2017	Reorganización de contenidos e incorporación de nuevos requisitos base definidos por el CA/Browser fórum.
5.3	13/06/2018	Incorporación de requisitos conforme estándares ETSI y RGPD.
5.4	5/03/2019	Incorporación de la jerarquía de AC raíz Servidores Seguros
5.5	05/11/2019	Incorporación de la jerarquía de AC Sector Público y AC Unidades de Sellado de Tiempo. Revisión general y actualización de mejora

Versión	Fecha	Descripción
5.6	06/02/2020	Incorporación de aspectos relativos al servicio de información sobre el estado de los certificados e información al respecto del servicio de firma en servidor.
5.7	16/06/2020	Revisión general
5.8	29/09/2020	Incorporación de aspectos relativos al servicio online de información sobre el estado de los certificados y derechos de propiedad intelectual
5.9	18/02/2021	Revisión de cumplimiento Ley 6/2020. Se documenta el intervalo máximo entre dos revisiones de la Política de Seguridad de la Información.
5.10	28/04/2021	Revisión Política Mozilla v2.7.1. – Se incorpora información en relación a los métodos para comunicar un compromiso de claves. Se elimina la información relativa a la raíz AC Servidores Seguros dado que ya se incluye en su propia DPC
5.11	02/03/2022	Incorporación de información para las terceras partes que confían en certificados cualificados.
5.12	02/06/2022	Se incluye la información del estado “Caducado” para el certificado de la AC Subordinada Administración Pública
5.13	15/02/2023	Revisión aptos. 6.2.1 y 9.17. Se amplía la información sobre los módulos criptográficos y procedimiento por pérdida de certificación QSCD.
5.14	24/03/2023	Revisión general normativa y legislación de aplicación para el servicio video identificación. Modificación de las referencias al nuevo estatuto RD 51/2023 y revisión del apto. 8.
5.15	07/07/2023	Actualización de puntos de distribución de CRLs en AC Subordinada Usuarios.
6.0	28/08/2023	Revisión general conforme a S/MIME Baseline Requirements v.1.0.1 y el estándar ETSI TS 119 411-6 para la emisión de certificados con correo electrónico seguro
6.1	11/04/2024	Actualización de la extensión “Certificate Policies”
6.2	05/02/2025	Revisión general. Inclusión nueva jerarquía

Versión	Fecha	Descripción
7.0	05/03/2025	Revisión general. Incorporación de nuevas SubCAs
7.1	18/12/2025	Incorporación nueva Subordinada de la AC FNMT-Raíz
7.2	29/01/2026	Actualización apartado 9.17

Referencia: DPC/DGPC0702/SGPSC/2026

Documento clasificado como: *Público*

Índice de contenidos

1. Introducción 13

1.1. Objeto 14

1.2. Nombre del documento e identificación 14

1.3. Partes intervinientes 15
1.3.1. Autoridades de Certificación 15
1.3.1.1. Algoritmo de Firma 21
1.3.2. Autoridad de Registro 23
1.3.3. Suscriptores de los certificados 23
1.3.4. Partes que confían 23
1.3.5. Otros participantes 23
1.3.5.1. Autoridad de Sellado de Tiempo 23

1.4. Uso de los certificados 23
1.4.1. Usos permitidos de los certificados 23
1.4.2. Restricciones en el uso de los certificados 24

1.5. Administración de Políticas 24
1.5.1. Entidad responsable 24
1.5.2. Datos de contacto 24
1.5.3. Responsables de adecuación de la DPC 25
1.5.4. Procedimiento de aprobación de la DPC 25

1.6. Definiciones y Acrónimos 26
1.6.1. Definiciones 26
1.6.2. Acrónimos 35

2. Publicación y repositorios 36

2.1. Repositorio 36

2.2. Publicación de información de certificación 36

2.3. Frecuencia de publicación 37

2.4. Control de acceso a los repositorios 37

3. Identificación y autenticación 37

3.1. Nombres 37
3.1.1. Tipos de nombres 37
3.1.2. Significado de los nombres 37
3.1.3. Seudónimos 37
3.1.4. Reglas utilizadas para interpretar varios formatos de nombres 38
3.1.5. Unicidad de los nombres 38
3.1.6. Reconocimiento y autenticación de marcas registradas 38

3.2. Validación inicial de la identidad 38
3.2.1. Métodos para probar la posesión de la clave privada 38
3.2.2. Autenticación de la identidad de la organización 39
3.2.3. Autenticación de la identidad de la persona física solicitante 39
3.2.4. Información no verificada del Suscriptor 39

3.2.5. Validación de la Autoridad 39
3.2.6. Criterios de interoperación 39

3.3. Identificación y autenticación para peticiones de renovación de claves 39
3.3.1. Renovación rutinaria 39
3.3.2. Renovación después de una revocación 39

3.4. Identificación y autenticación para peticiones de revocación 40

4. Requisitos operativos del ciclo de vida de los certificados 40

4.1. Solicitud de Certificados 40
4.1.1. Quién puede solicitar un Certificado 40
4.1.2. Proceso de registro y responsabilidades 40

4.2. Procedimiento de solicitud de certificados 40
4.2.1. Realización de las funciones de identificación y autenticación 40
4.2.2. Aprobación o rechazo de la solicitud del certificado 40
4.2.3. Tiempo en procesar la solicitud 41

4.3. Emisión del certificado 41
4.3.1. Acciones de la AC durante la emisión 41
4.3.2. Notificación al suscriptor 41

4.4. Aceptación del certificado 41
4.4.1. Proceso de aceptación 41
4.4.2. Publicación del certificado por la AC 41
4.4.3. Notificación de la emisión a otras entidades 41

4.5. Par de claves y uso del certificado 41
4.5.1. Clave privada del suscriptor y uso del certificado 41
4.5.2. Uso del certificado y la clave pública por terceros que confían 42

4.6. Renovación del certificado 42
4.6.1. Circunstancias para la renovación del certificado 42
4.6.2. Quién puede solicitar la renovación del certificado 42
4.6.3. Procesamiento de solicitudes de renovación del certificado 42
4.6.4. Notificación de la renovación del certificado 42
4.6.5. Conducta que constituye la aceptación de la renovación del certificado 42
4.6.6. Publicación del certificado renovado 42
4.6.7. Notificación de la renovación del certificado a otras entidades 42

4.7. Renovación con regeneración de las claves del certificado 43
4.7.1. Circunstancias para la renovación con regeneración de claves 43
4.7.2. Quién puede solicitar la renovación con regeneración de claves 43
4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves 43
4.7.4. Notificación de la renovación con regeneración de claves 43
4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves 43
4.7.6. Publicación del certificado renovado 43
4.7.7. Notificación de la renovación con regeneración de claves a otras entidades 43

4.8. Modificación del certificado 43
4.8.1. Circunstancias para la modificación del certificado 43
4.8.2. Quién puede solicitar la modificación del certificado 44
4.8.3. Procesamiento de solicitudes de modificación del certificado 44

4.8.4. Notificación de la modificación del certificado 44
4.8.5. Conducta que constituye la aceptación de la modificación del certificado 44
4.8.6. Publicación del certificado modificado 44
4.8.7. Notificación de la modificación del certificado a otras entidades 44

4.9. Revocación del certificado 44
4.9.1. Circunstancias para la revocación 44
4.9.2. Quién puede solicitar la revocación 44
4.9.3. Procedimiento de solicitud de la revocación 45
4.9.4. Periodo de gracia de la solicitud de revocación 45
4.9.5. Plazo de tiempo para procesar la solicitud de revocación 45
4.9.6. Obligación de verificar las revocaciones por las partes que confían 45
4.9.7. Frecuencia de generación de CRLs 45
4.9.8. Periodo máximo de latencia de las CRLs 45
4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados 45
4.9.10. Requisitos de comprobación en línea de la revocación 46
4.9.11. Otras formas de aviso de revocación disponibles 46
4.9.12. Requisitos especiales de revocación de claves comprometidas 46
4.9.13. Circunstancias para la suspensión 46
4.9.14. Quién puede solicitar la suspensión 46
4.9.15. Procedimiento para la petición de la suspensión 47
4.9.16. Límites sobre el periodo de suspensión 47

4.10. Servicios de información del estado de los certificados 47
4.10.1. Características operativas 51
4.10.2. Disponibilidad del servicio 51
4.10.3. Características opcionales 51

4.11. Finalización de la suscripción 52

4.12. Custodia y recuperación de claves 52
4.12.1. Prácticas y políticas de custodia y recuperación de claves 52
4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión 52

5. Controles de seguridad física, de procedimientos y de personal 52

5.1. Controles de Seguridad Física 53
5.1.1. Ubicación de las instalaciones 53
5.1.1.1. Situación del Centro de Proceso de Datos 53
5.1.2. Acceso Físico 54
5.1.2.1. Perímetro de seguridad física 54
5.1.2.2. Controles físicos de entrada 54
5.1.2.3. El trabajo en áreas seguras 54
5.1.2.4. Visitas 55
5.1.2.5. Áreas aisladas de carga y descarga 55
5.1.3. Electricidad y Aire Acondicionado 55
5.1.3.1. Seguridad del cableado 55
5.1.4. Exposición al agua 55
5.1.5. Prevención y Protección contra incendios 55
5.1.6. Almacenamiento de Soportes 56
5.1.6.1. Recuperación de la información 56
5.1.7. Eliminación de Residuos 56
5.1.8. Copias de Seguridad fuera de las instalaciones 56

5.2. Controles de Procedimiento ... *56*
5.2.1. Roles de confianza ... 57
5.2.2. Número de personas por tarea ... 58
5.2.3. Identificación y autenticación para cada rol ... 58
5.2.4. Roles que requieren segregación de funciones ... 58

5.3. Controles de Personal ... *58*
5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos ... 60
5.3.2. Procedimientos de verificación de antecedentes ... 60
5.3.3. Requisitos de formación ... 60
5.3.4. Requisitos y frecuencia de actualización formativa ... 61
5.3.5. Secuencia y frecuencia de rotación laboral ... 61
5.3.6. Sanciones por acciones no autorizadas ... 61
5.3.7. Requisitos de contratación de personal ... 62
5.3.7.1. Requisitos de contratación de terceros ... 62
5.3.8. Suministro de documentación al personal ... 62

5.4. Procedimientos de auditoría ... *63*
5.4.1. Tipos de eventos registrados ... 63
5.4.1.1. Registro o Log de actividades con Firewall y enrutadores ... 65
5.4.2. Frecuencia de procesamiento de registros ... 65
5.4.3. Periodo de conservación de los registros ... 65
5.4.4. Protección de los registros ... 66
5.4.5. Procedimientos de copias de seguridad de los registros auditados ... 66
5.4.6. Sistema de recolección de registros ... 66
5.4.7. Notificación al sujeto causante de los eventos ... 66
5.4.8. Análisis de vulnerabilidades ... 66

5.5. Archivado de registros ... *66*
5.5.1. Tipos de registros archivados ... 66
5.5.2. Periodo de retención del archivo ... 67
5.5.3. Protección del archivo ... 67
5.5.4. Procedimientos de copia de respaldo del archivo ... 68
5.5.5. Requisitos para el sellado de tiempo de los registros ... 68
5.5.6. Sistema de archivo ... 68
5.5.7. Procedimientos para obtener y verificar la información archivada ... 68

5.6. Cambio de claves de la AC ... *69*

5.7. Gestión de incidentes y vulnerabilidades ... *69*
5.7.1. Gestión de incidentes y vulnerabilidades ... 69
5.7.2. Actuación ante datos y software corruptos ... 69
5.7.3. Procedimiento ante compromiso de la clave privada de la AC ... 69
5.7.4. Continuidad de negocio después de un desastre ... 70

5.8. Cese de la actividad del Prestador de Servicios de Confianza ... *71*

6. Controles de seguridad técnica ... 72

6.1. Generación e instalación de las Claves ... *72*
6.1.1. Generación del par de Claves ... 72
6.1.1.1. Generación del par de Claves de la CA ... 72
6.1.1.2. Generación del par de Claves de la RA ... 73
6.1.1.3. Generación del par de Claves de los Suscriptores ... 73

6.1.2. Envío de la clave privada al suscriptor ... 73
6.1.3. Envío de la clave pública al emisor del certificado ... 73
6.1.4. Distribución de la clave pública de la AC a las partes que confían ... 73
6.1.5. Tamaños de claves y algoritmos utilizados ... 73
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad ... 74
6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3) ... 74

6.2. Protección de la clave privada y controles de los módulos criptográficos ... 74
6.2.1. Estándares para los módulos criptográficos ... 74
6.2.2. Control multi-persona (n de m) de la clave privada ... 75
6.2.3. Custodia de la clave privada ... 75
6.2.4. Copia de seguridad de la clave privada ... 75
6.2.5. Archivado de la clave privada ... 75
6.2.6. Trasferencia de la clave privada a o desde el módulo criptográfico ... 76
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico ... 76
6.2.8. Método de activación de la clave privada ... 76
6.2.9. Método de desactivación de la clave privada ... 76
6.2.10. Método de destrucción de la clave privada ... 77
6.2.11. Clasificación de los módulos criptográficos ... 77

6.3. Otros aspectos de la gestión del par de claves ... 77
6.3.1. Archivo de la clave pública ... 77
6.3.2. Periodos de operación del certificado y periodos de uso del par de claves ... 77

6.4. Datos de activación ... 78
6.4.1. Generación e instalación de datos de activación ... 78
6.4.2. Protección de datos de activación ... 78
6.4.3. Otros aspectos de los datos de activación ... 78

6.5. Controles de seguridad informática ... 78
6.5.1. Requisitos técnicos específicos de seguridad informática ... 78
6.5.1.1. Comunicación de las incidencias de seguridad ... 78
6.5.1.2. Comunicación de las debilidades de seguridad ... 79
6.5.1.3. Comunicación de los fallos del software ... 79
6.5.1.4. Aprendiendo de las incidencias ... 79
6.5.2. Evaluación del nivel de seguridad informática ... 79

6.6. Controles técnicos del ciclo de vida ... 79
6.6.1. Controles de desarrollo de sistemas ... 79
6.6.2. Controles de gestión de la seguridad ... 80
6.6.3. Controles de seguridad del ciclo de vida ... 80
6.6.3.1. Actualización de algoritmia ... 80

6.7. Controles de seguridad de la red ... 80

6.8. Fuente de tiempo ... 81

6.9. Otros controles adicionales ... 81
6.9.1. Control de la capacidad de prestación de los servicios ... 81
6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas ... 82

7. Perfiles de los certificados, CRLs y OCSP ... 82

7.1. Perfil del certificado ... 82
7.1.1. Número de versión ... 82

7.1.2. Extensiones del certificado 82
7.1.3. Identificadores de objeto de algoritmos 82
7.1.4. Formatos de nombres 82
7.1.5. Restricciones de nombres 83
7.1.6. Identificador de objeto de política de certificado 83
7.1.7. Empleo de la extensión restricciones de política 83
7.1.8. Sintaxis y semántica de los calificadores de política 83
7.1.9. Tratamiento semántico para la extensión "certificate policy" 83

7.2. Perfil de la CRL 83
7.2.1. Número de versión 83
7.2.2. CRL y extensiones 84

7.3. Perfil de OCSP 86
7.3.1. Número de versión 86
7.3.2. Extensiones del OCSP 86

8. Auditorías de cumplimiento 86

8.1. Frecuencia de las auditorías 88

8.2. Cualificación del auditor 88

8.3. Relación del auditor con la empresa auditada 88

8.4. Elementos objetos de auditoría 88

8.5. Toma de decisiones frente a detección de deficiencias 89

8.6. Comunicación de los resultados 89

8.7. Autoevaluación 89

9. Otros asuntos legales y de actividad 89

9.1. Tarifas 89
9.1.1. Tarifas de acceso a los certificados 90
9.1.2. Tarifas de acceso a la información de estado o revocación 90
9.1.3. Tarifas para otros servicios 90
9.1.4. Política de reembolso 90

9.2. Responsabilidades financieras 90
9.2.1. Seguro de responsabilidad civil 91
9.2.2. Otros activos 91
9.2.3. Seguros y garantías para entidades finales 91

9.3. Confidencialidad de la información 91
9.3.1. Alcance de la información confidencial 91
9.3.2. Información no incluida en el alcance 91
9.3.3. Responsabilidad para proteger la información confidencial 91

9.4. Protección de datos personales 92
9.4.1. Plan de privacidad 92
9.4.2. Información tratada como privada 92
9.4.3. Información no considerada privada 92
9.4.4. Responsabilidad de proteger la información privada 92

9.4.4.1. Delegado de Protección de Datos 93
9.4.4.2. Registro de actividades de tratamiento 93
9.4.4.3. Derechos de los interesados 93
9.4.4.4. Cooperación con las Autoridades 93
9.4.4.5. Notificación de violaciones de seguridad 94
9.4.5. Aviso y consentimiento para usar información privada 94
9.4.6. Divulgación conforme al proceso judicial o administrativo 94
9.4.7. Otras circunstancias de divulgación de información 94

9.5. Derechos de propiedad intelectual 94

9.6. Obligaciones y garantías 95
9.6.1. Obligaciones de la AC 96
9.6.1.1. Con carácter previo a la emisión del Certificado 96
9.6.1.2. Identificación del Titular 96
9.6.1.3. Generación de Datos de creación de Firma e información adicional 96
9.6.1.4. Conservación de la información por la FNMT-RCM 97
9.6.1.5. Protección de los Datos de Carácter Personal 97
9.6.2. Obligaciones de la AR 97
9.6.3. Obligaciones de los titulares 98
9.6.4. Obligaciones de las partes que confían 99
9.6.5. Obligaciones de otros participantes 100

9.7. Renuncia de garantías 100

9.8. Limitaciones de responsabilidad 101

9.9. Indemnizaciones 102
9.9.1. Indemnización de la CA 102
9.9.2. Indemnización de los Suscriptores 102
9.9.3. Indemnización de las partes que confían 102

9.10. Periodo de validez de este documento 103
9.10.1. Plazo 103
9.10.2. Terminación 103
9.10.3. Efectos de la finalización 103

9.11. Notificaciones individuales y comunicación con los participantes 103

9.12. Modificaciones de este documento 103
9.12.1. Procedimiento para las modificaciones 103
9.12.2. Periodo y mecanismo de notificación 104
9.12.3. Circunstancias bajo las cuales debe cambiarse un OID 104

9.13. Reclamaciones y resolución de disputas 104

9.14. Normativa de aplicación 104

9.15. Cumplimiento de la normativa aplicable 106

9.16. Estipulaciones diversas 106
9.16.1. Acuerdo integro 106
9.16.2. Asignación 106
9.16.3. Severabilidad 106
9.16.4. Cumplimiento 106
9.16.5. Fuerza Mayor 106

9.17. Otras estipulaciones 107

Anexo I: Perfil del certificado raíz FNMT 109

Anexo II: Perfil del certificado raíz FNMT G2 111

Anexo III: Perfil del certificado raíz FNMT TSA 113

Índice de tablas

Tabla 1 – Certificado RAIZ FNMT-RCM 15
Tabla 2 – Certificado RAIZ FNMT-RCM G2 16
Tabla 3 – Perfil de la CRL de la AC RAÍZ FNMT-RCM 84
Tabla 4 – Perfil de la CRL de la AC RAÍZ FNMT-RCM G2 84
Tabla 4 – Perfil de la CRL de la AC RAÍZ FNMT-RCM TSA 85

Índice de figuras

Figura-1: Jerarquía de AC RAIZ FNMT 19
Figura-2: Jerarquía de AC RAIZ FNMT G2 20
Figura-3: Jerarquía de AC RAIZ FNMT-RCM TSA 21

1. INTRODUCCIÓN

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

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

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

4. La 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.

5. La FNMT-RCM está acreditada como *Prestador cualificado de servicios de confianza* de conformidad con el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

6. El objetivo de la FNMT-RCM, a través de su Departamento CERES, es proporcionar una *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 adoptado coherente con el mencionado Reglamento eIDAS, con la legislación nacional, así como con la normativa específica de la propia FNMT-RCM.

7. 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.

8. 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.

1.1. OBJETO

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

   - la gestión de 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 electrónicos*, que se ofrecen como parte de la prestación del *Servicio de sellado de tiempo*.

10. Además, en el presente documento se recogen los detalles del régimen de responsabilidad aplicable a las partes usuarias y/o que confían en los servicios mencionados en el párrafo anterior, los controles de seguridad aplicados a sus procedimientos e instalaciones en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, y las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal, y demás cuestiones de tipo informativo que considere interesante poner a disposición del público.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

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

12. Este documento no trata los aspectos particulares de las diferentes *Prácticas y Políticas de certificación, del servicio de firma en servidor* o de *Sellado de tiempo* que la FNMT-RCM implementa para la prestación de servicios de confianza. Dichas particularidades se desarrollan en los correspondientes documentos teniendo, como marco general de aplicación, la presente DGPC.

13. 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 *DGPC*.

14. El Comité de Seguridad de la Información de la FNMT-RCM revisa regularmente los riesgos a los que se encuentra expuesta la Organización y aprueba los planes de tratamiento necesarios para garantizar la seguridad de los servicios definidos en cada una de las Políticas de Certificación.

15. 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.

16. 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

17. Estos procedimientos se basan principalmente en las normas del *European Telecommunications Standards Institute* (ETSI).

1.3. PARTES INTERVINIENTES

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

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

1.3.1. Autoridades de Certificación

19. La FNMT-RCM es la *Autoridad de Certificación* que expide los *Certificados* electrónicos conforme a la presente DGPC y de los que será objeto una determinada Declaración de Políticas de Certificación Particulares. A estos efectos, existen las siguientes Autoridades de Certificación:

a) Autoridades de Certificación raíz (Jerarquía RSA). Dichas Autoridades expiden exclusivamente *Certificados* de Autoridades de Certificación subordinadas con algoritmia RSA. Los certificados raíz de esta AC vienen identificados por la siguiente información:

Tabla 1 – Certificado RAIZ FNMT-RCM

CERTIFICADO RAIZ FNMT-RCM	
Sujeto	OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES

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

b) Autoridades de Certificación subordinadas a la raíz de RSA: expiden los *Certificados* de entidad final de los que será objeto una determinada Declaración de Políticas de Certificación Particulares.

c) Autoridades de Certificación raíz (Jerarquía Curva Elíptica). Dichas Autoridades expiden exclusivamente *Certificados* de Autoridades de Certificación subordinadas con algoritmia de curva elíptica. Los certificados raíz de esta AC vienen identificados por la siguiente información:

Tabla 2 – Certificado RAIZ FNMT-RCM G2

CERTIFICADO RAIZ FNMT-RCM G2	
Sujeto	CN=AC RAIZ FNMT-RCM G2, Org_ID=VATES-Q2826004J, O=FNMT-RCM, C=ES
Emisor	CN=AC RAIZ FNMT-RCM G2, Org_ID=VATES-Q2826004J, O=FNMT-RCM, C=ES
Número de serie (hex)	1F B6 4F 91 9E C5 01 EA B1 21 28 BB 11 7A 00 3C 7C 5A EF 1A
Validez	No antes:10 Octubre 2024 No después: 04 Octubre 2049

CERTIFICADO RAIZ FNMT-RCM G2	
Clave pública	ECC P-384
Algoritmo de firma	ecdsa-with-SHA384
Identificador de clave	E2 29 99 47 2A FF 5B 26 8A C8 34 41 66 45 AF 52 3A 08 F1 80

d) Autoridades de Certificación subordinadas a la raíz de curva elíptica: expiden los *Certificados* de entidad final de los que será objeto una determinada Declaración de Políticas de Certificación Particulares.

e) Autoridades de Certificación raíz TSA (Jerarquía Curva Elíptica). Dichas Autoridades expiden exclusivamente *Certificados* de Autoridades de Certificación subordinadas con algoritmia de curva elíptica que emitan unidades de sellado de tiempo. Los certificados raíz de esta AC vienen identificados por la siguiente información:

Tabla 3 – Certificado RAIZ FNMT-RCM TSA

CERTIFICADO RAIZ FNMT-RCM TSA	
Sujeto	CN=AC RAIZ FNMT-RCM TSA, Org_ID=VATES-Q2826004J, O=FNMT-RCM, C=ES
Emisor	CN=AC RAIZ FNMT-RCM TSA, Org_ID=VATES-Q2826004J, O=FNMT-RCM, C=ES
Número de serie (hex)	51 97 B0 DC 75 6F 57 72 7C 8E 41 DF C0 36 DE BB 88 3E 05 EF
Validez	No antes:10 Octubre 2024 No después: 04 Octubre 2049
Clave pública	ECC P-384
Algoritmo de firma	ecdsa-with-SHA384
Identificador de clave	8F 18 75 3B 80 43 DC 18 C1 6E E3 B4 B6 6A AC F7 37 66 09 01

f) Autoridades de Certificación subordinadas a la raíz de curva elíptica TSA: expiden las Unidades de *Sellado de Tiempo* de los que será objeto una determinada Declaración de Políticas de Certificación Particulares.

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

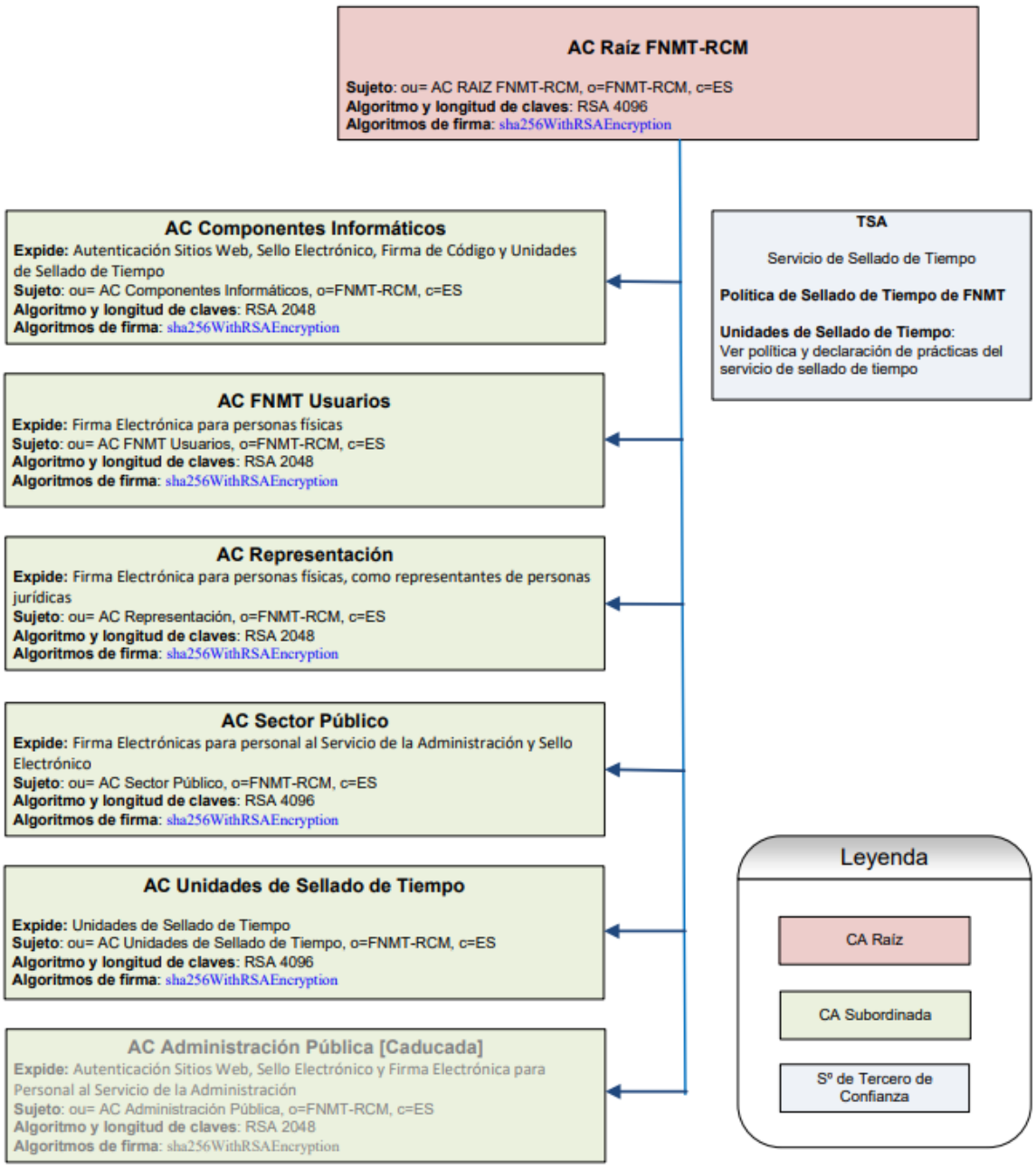

Figura-1: Jerarquía de AC RAIZ FNMT

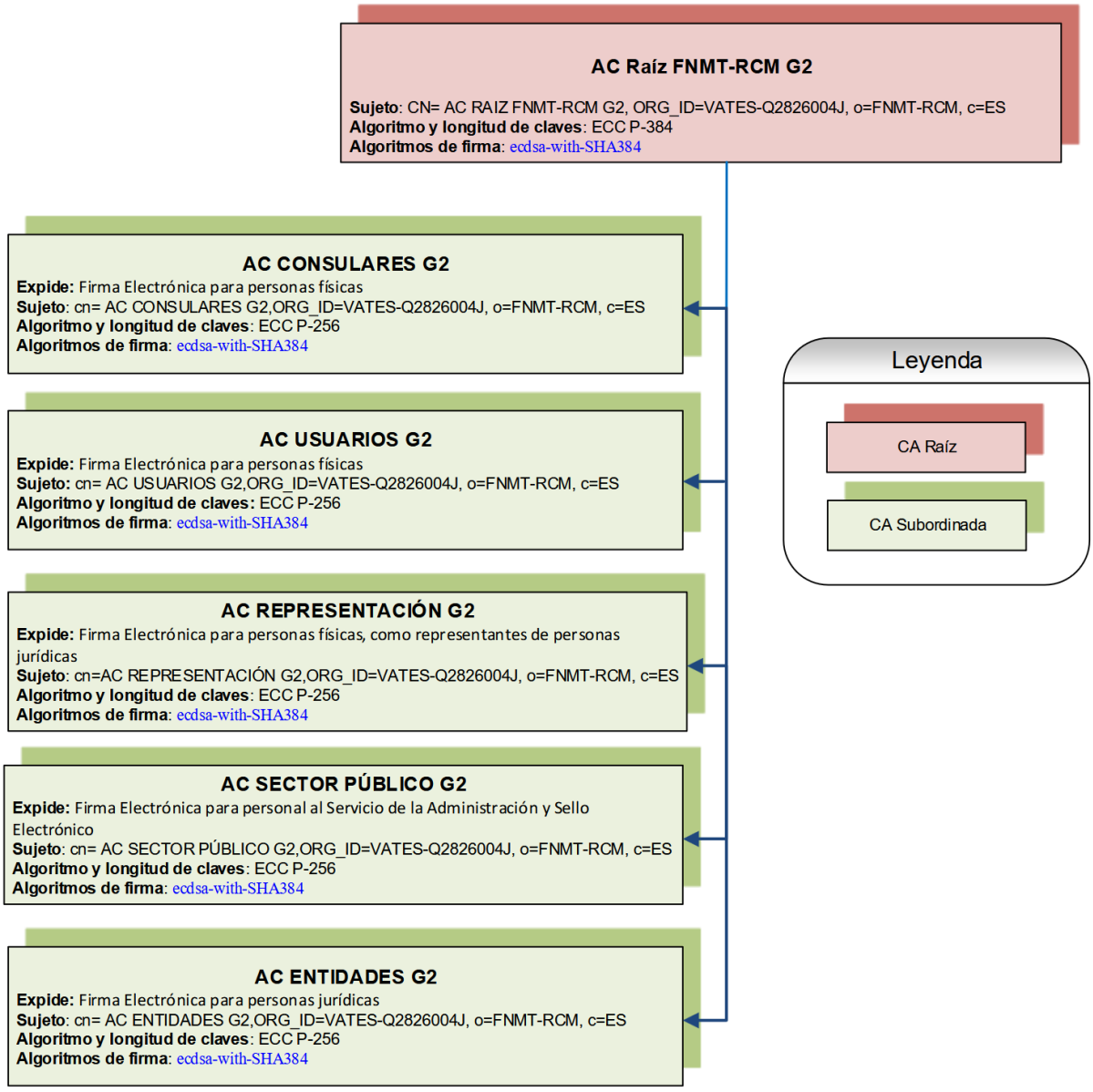

Figura-2: Jerarquía de AC RAIZ FNMT G2

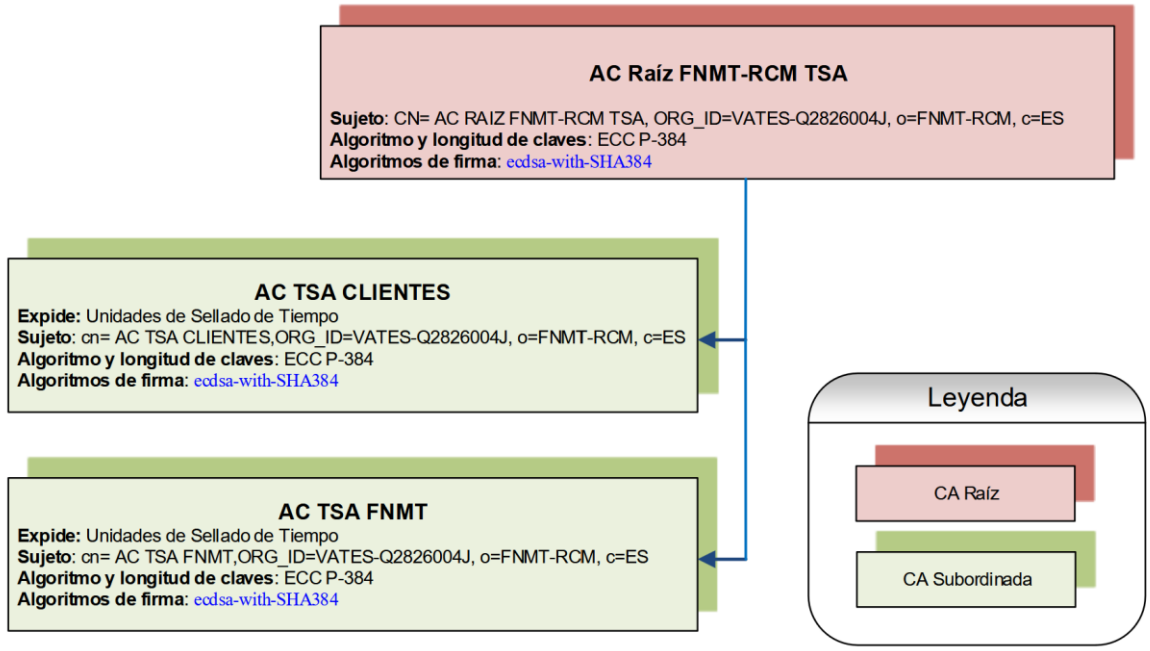

Figura-3: Jerarquía de AC RAIZ FNMT-RCM TSA

21. 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.

22. 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).

23. Por razones de interoperabilidad y previsiones de futuro, los *Datos de Creación de Firma / Sello* de estas *Autoridades de Certificación* han sido autofirmados con algoritmos diferentes. Así pues, se publica la siguiente información:

1.3.1.1. Algoritmo de Firma

24. **Información relativa al *Certificado* "AC RAIZ FNTM-RCM":**

- pkcs1-sha1WithRSAEncryption,
- pkcs1-sha256WithRSAEncryption,
- pkcs1-sha512WithRSAEncryption

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

25. **Información relativa al *Certificado* "AC RAIZ FNTM-RCM G2":**

Clave ECC P-384

- Número de serie: 0x1FB64F919EC501EAB12128BB117A003C7C5AEF1A
- Huella Digital (SHA-1): A4:D6:B7:70:E7:65:A9:BF:17:EC:D7:B5:E0:3B:85:2D:61:2F:A7:1D
- Huella Digital (SHA-256): 02:07:86:53:9F:02:B6:23:CF:DF:32:5B:2E:4E:45:E0:D9:E3:F1:B8:E5:EC:96:00:EB:F0:AC:8F:BF:03:FB:E2
- Huella Digital (MD5): 21:2C:F3:94:5A:90:E9:A6:A2:8B:86:62:40:E9:76:DC
- 7F:73:3A:00:2E:DF:E0

26. **Información relativa al *Certificado* "AC RAIZ FNTM-RCM TSA":**

Clave ECC P-384

- Número de serie: 0x5197B0DC756F57727C8E41DFC036DEBB883E05EF
- Huella Digital (SHA-1): E9:0D:1A:8F:04:E0:D4:A1:31:BF:4E:7E:E2:BC:57:AE:7A:8A:93:E4
- Huella Digital (SHA-256): 95:69:94:8C:A1:21:D3:C7:A1:D0:7B:D1:DD:7E:1D:48:EA:7A:5B:1E:E3:E7:E9:55:7C:06:C3:B8:B2:8C:02:3E
- Huella Digital (MD5): 6D:E9:15:7F:E2:A5:3E:CC:C6:B5:43:5B:4B:2F:87:9E

1.3.2. Autoridad de Registro

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

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

1.3.3. Suscriptores de los certificados

29. El *Suscriptor* de un *Certificado* puede ser una entidad diferente de la figura de *Firmante* cuando hay una relación de representación o pertenencia a una Organización, de forma que ésta última es considerada la entidad *Suscriptora*, o cuando se trate de *Certificados* de *Sello electrónico* o de *Autenticación web*. No obstante, cada Declaración de Políticas de Certificación Particulares determinará esta posible separación entre las figuras del *Firmante* y el *Suscriptor*.

30. Los Firmantes son las personas físicas que mantienen bajo su uso exclusivo los *Datos de creación de firma* asociados a los *Certificados* de los que son *Titulares*.

1.3.4. Partes que confían

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

1.3.5. Otros participantes

1.3.5.1. Autoridad de Sellado de Tiempo

32. La FNMT-RCM es la *Autoridad de Sellado de Tiempo* cuando provee el *Servicio de Confianza* de creación de *Sellos de tiempo electrónicos*, bajo su correspondiente Declaración de Prácticas Particulares.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

33. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

1.4.2. Restricciones en el uso de los certificados

34. No se podrán emplear los *Certificados* de entidad final expedidos por la FNMT-RCM para:

- Firmar o sellar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Usos particulares o privados, salvo para relacionarse con las Administraciones cuando éstas lo admitan.
- Firmar o sellar software o componentes a excepción de los *Certificados de componente de firma de código*
- Generar sellos de tiempo para procedimientos de Fechado electrónico a excepción de los *Certificados* expedidos por la FNMT-RCM para *Unidades de Sellado de Tiempo*.
- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como por ejemplo serían a título enunciativo:
  - Prestar servicios de OCSP.
  - Generar Listas de Revocación.
  - Prestar servicios de notificación.

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

35. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, con NIF Q2826004-J, es la Autoridad de Certificación que expide los certificados a los que aplica esta *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)*.

1.5.2. Datos de contacto

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

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

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: ceres@fnmt.es

Teléfono: +34 91 740 69 82

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

1.5.3. Responsables de adecuación de la DPC

38. La Dirección de la FNMT-RCM dispone, dentro de sus competencias, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y mantenimiento, tanto para la presente *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, como para las Prácticas de Certificación Particulares y la Política de Certificación correspondiente.

1.5.4. Procedimiento de aprobación de la DPC

39. 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.

40. La FNMT-RCM dispone de *Políticas y Prácticas de los servicios de confianza* que presta, específicas para cada tipo de *Certificado* o servicio de confianza. En particular, declara que:

- La FNMT-RCM tiene capacidad para especificar, revisar, y aprobar las *Políticas de Certificación* y de sus servicios de confianza a través de su Dirección General y demás órganos directivos de la misma.
- La FNMT-RCM dispone de unas *Prácticas de Servicio de confianza Particulares* en las que se detallan las prácticas aplicables a los servicios identificados en cada *Política de* dicho servicio.
- 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, y del servicio de firma en servidor,* 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*.
- Cualquier modificación en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* o en las *Políticas* y *Prácticas de Certificación Particulares* será publicada de forma inmediata en la URL de acceso a las mismas.

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

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

42. No obstante, a los efectos de lo dispuesto en la presente Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica 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:

- *Acuerdos: Contratos, Encomiendas, Encargos* y/o *Convenios* empleados como 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.
- *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 Confianza*, responsable de emitir y revocar los *Certificados*, utilizados en la *Firma electrónica*. Jurídicamente es un caso particular de *Prestador de Servicios de Confianza* 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 Confianza*, responsable de emitir *Sellos de tiempo electrónico*. Jurídicamente es un caso particular de *Prestador de Servicios de Confianza* 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.
- *Certificado de autenticación*: Certificado que permite garantizar electrónicamente y acreditar la identidad de una persona física o jurídica ante servicios y aplicaciones informáticas.
- *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 de firma electrónica*: Una declaración electrónica que vincula los *Datos de validación* de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.
- *Certificado de sello electrónico*: Una declaración electrónica que vincula los *Datos de validación* de un sello con una persona jurídica y confirma el nombre de esa persona.

- *Certificado raíz FNMT*: 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 cualificado de firma electrónica*: *Certificado* electrónico emitido por un *Prestador de Servicios de Confianza* cumpliendo los requisitos establecidos en el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, así como en la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza, 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 confianza 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* 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*: Conjunto de personas y entidades que se relacionan con *Certificados* entre sí, bajo el marco general de la presente *Declaración General de Prácticas de* Servicios de Confianza y de Certificación electrónica, y particular de los correspondientes convenios y/o contratos que hayan suscrito, directamente o a través de representantes, con la FNMT-RCM.
- *Confidencialidad*: Cualidad que supone que la información no es accesible o no ha sido revelada a personas, entidades o procesos no autorizados.
- *CPD*: Centro de Proceso de Datos.
- *Creador del sello*: Es una persona jurídica que crea un *Sello electrónico*.

- *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 creación de sello:* Los datos únicos que utiliza el *Creador del sello electrónico* para crearlo.
- *Datos de verificación / validación de firma o de sello*: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar firmas o sellos electrónicos. 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 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*.
- *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* o *DGPC:* 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 Confianza* y en cumplimiento del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- *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 cualificado de creación de firma (DCCF)*: Elemento que sirve para aplicar los *Datos de creación de Firma*, que cumple con los requisitos establecidos en el Anexo II del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- *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.
- *EIT*: Técnicas y medios electrónicos, informáticos y telemáticos.
- *Entidad usuaria*: Aquella persona, entidad pública o privada que ha firmado un *Contrato*, *Encomienda, Encargo* o *Convenio* con la FNMT-RCM para actuar en la *Comunidad Electrónica*.
- *Firma electrónica*: Datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el *Firmante* para firmar.
- *Firma electrónica avanzada*: Es aquella *Firma electrónica* que está vinculada al *Firmante* de manera única, permite identificar al *Firmante,* ha sido creada utilizando *Datos de creación de firma electrónica* que el *Firmante* puede utilizar con un alto nivel de confianza bajo su control exclusivo, y que está vinculada con los datos firmados de modo tal que cualquier modificación ulterior de los mismos es detectable.
- *Firma electrónica cualificada*: Es aquella *Firma electrónica avanzada* basada en un *Certificado cualificado de firma electrónica* y generada mediante un *Dispositivo cualificado de creación de firma*.
- *Firmante*: La persona física que crea una firma electrónica en nombre propio o en nombre de una persona jurídica o Entidad sin personalidad 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.
- *Informe de incidencia sobre certificado:* queja de sospecha de compromiso clave, mal uso del certificado u otros tipos de fraude, compromiso, mal uso o conducta inapropiada relacionada con los certificados.
- *Infraestructura de Claves Públicas* (PKI, *public key infrastructure*): 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.
- *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 Confianza*: 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*.
- *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.
- *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.
- *Política y Prácticas del servicio de firma en servidor:* Documento que establece el conjunto de reglas y procedimientos específicos seguidos por la FNMT-RCM para la prestación de su servicio de firma electrónica en servidor.
- *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 Confianza:* Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza, de conformidad con lo establecido en el REGLAMENTO

(UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

- *Prestador cualificado de servicios de confianza*: *Prestador de Servicios de Confianza* que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.
- *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*.
- *QSCD (Qualified Signature Creation Device):* Véase *Dispositivo cualificado de creación de firma.*
- *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 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*: RFC 3161 – *"Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)",* que logra fechar el documento de forma objetiva.
- *Sello de tiempo electrónico:* Datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.
- *Sello electrónico*: Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.
- *Sello electrónico avanzado*: Es un *Sello electrónico* que está vinculado al *Creador del sello* de manera única, permite identificar al *Creador del sello,* ha sido creado utilizando *Datos de creación de sello electrónico* que el *Creador del sello* puede utilizar con un alto nivel de confianza bajo su control exclusivo, y que está vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos es detectable.
- *Sello electrónico cualificado*: Es un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.
- *Servicio de información y consulta sobre el estado de validez de los certificados*: Servicio prestado por la FNMT-RCM a los interesados por el cual se proporciona información sobre el estado de los *Certificados* por los que el usuario se interesa.

- *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 EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*", 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.
- *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.
- *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 F*irma electrónica* con los *Datos de Creación de Firma* albergados en su interior. La Tarjeta Criptográfica puede ser un DCCF si cumple lo especificado en su definición.
- *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 Confianza*. 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 sello para la emisión de *Sellos de tiempo electrónicos*.
- *Usuario* (de un servicio) o *Parte usuaria*: La persona física o jurídica que confía en la identificación electrónica o el servicio de confianza.
- *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".

1.6.2. Acrónimos

43. A los efectos de lo dispuesto en la presente Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y, en su caso, las Declaraciones de Certificación Particulares dependientes de esta, son de aplicación los siguientes acrónimos, cuyo significado es acorde con el estándar europeo ETSI EN 319 411 "Policy and security requirements for Trust Service Providers issuing certificates":

CRL: Lista de *Certificados* revocados

DVC: *Certificado* de Validación de Dominio

EV: Validación Extendida

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

NCP: Política de *Certificado* Normalizado

NCP+: Política de *Certificado* Normalizado Extendida

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

OID: Identificador de Objeto (Object Identifier)

OVC: *Certificado* de validación de Organización

PSC: *Prestador de Servicios de Confianza*

SBR: CA/Browser Forum "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (S/MIME Baseline Requirements (SBR))

S/MIME: Secure MIME (Multipurpose Internet Mail Extensions) (Extensiones seguras para correo electrónico multipropósito)

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

UTC: Tiempo coordinado universal (Coordinated Universal Time).

2. PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIO

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

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

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

45. Adicionalmente, la FNMT-RCM mantiene los siguientes repositorios de información:

a. *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* 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)

1. Certificado de la AC RAIZ FNMT
   - Certificado de AC Subordinada Componentes Informáticos
   - Certificado de la AC Subordinada Representación
   - Certificado de la AC Subordinada Usuarios
   - Certificado de la AC Subordinada Sector Público
   - Certificado de la AC Subordinada Unidades de Sellado de Tiempo
   - Certificado de AC Subordinada Administración Públicas [Caducado]
   - Certificado cruzado de AC Raíz FNMT-RCM Servidores Seguros G2R
2. Certificado de la AC RAIZ FNMT G2
   - Certificado de la AC Subordinada Consulares G2
   - Certificado de la AC Subordinada Entidades G2
   - Certificado de la AC Subordinada Representación G2
   - Certificado de la AC Subordinada Usuarios G2
   - Certificado de la AC Subordinada Sector Público G2
3. Certificado de la AC RAIZ FNMT TSA
   - Certificado de AC Subordinada TSA FNMT
   - Certificado de AC Subordinada TSA CLIENTES

2.3. FRECUENCIA DE PUBLICACIÓN

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

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

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

49. La codificación de los *Certificados* sigue el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",

3.1.1. Tipos de nombres

50. Los *Certificados* electrónicos de entidad final contienen un nombre distintivo (*DN*) en el campo Subject Name, que se componen según se describe en la información relativa al perfil de cada tipo de *Certificado*. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.1.2. Significado de los nombres

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

3.1.3. Seudónimos

52. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.5. Unicidad de los nombres

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

3.1.6. Reconocimiento y autenticación de marcas registradas

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

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

56. Sin perjuicio de lo que pudieran establecer las correspondientes 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*.

57. 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*.

58. 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.

59. 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.

3.2.1. Métodos para probar la posesión de la clave privada

60. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.2.2. Autenticación de la identidad de la organización

61. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.2.3. Autenticación de la identidad de la persona física solicitante

62. A estos efectos, 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 admitidos y de comprobación de las cualidades del *Titular* que aporten las garantías suficientes de la veracidad de los datos.

63. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.2.4. Información no verificada del Suscriptor

64. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.2.5. Validación de la Autoridad

65. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.2.6. Criterios de interoperación

66. No existen relaciones de interactividad con Autoridades de Certificación externas a FNMT-RCM, sin perjucio del deber de colaboración establecido en las normas aplicables.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

3.3.1. Renovación rutinaria

67. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

3.3.2. Renovación después de una revocación

68. El proceso de renovación del *Certificado* tras la revocación del mismo será el mismo que el que se sigue en la emisión inicial de dicho *Certificado*.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

69. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

70. 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.

71. 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. Esto no será de aplicación en el caso de expedición de *Certificados de Firma Centralizada*, de conformidad con la normativa de aplicación.

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

72. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.1.2. Proceso de registro y responsabilidades

73. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

74. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.2.1. Realización de las funciones de identificación y autenticación

75. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.2.2. Aprobación o rechazo de la solicitud del certificado

76. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.2.3. Tiempo en procesar la solicitud

77. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

78. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.3.2. Notificación al suscriptor

79. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

80. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.4.2. Publicación del certificado por la AC

81. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.4.3. Notificación de la emisión a otras entidades

82. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

83. Aquellos aspectos relativos a las claves del *Prestador de Servicios de Confianza* se describen en el apartado “6.1 Generación e instalación de las claves”.

4.5.1. Clave privada del suscriptor y uso del certificado

84. En relación con las claves de los *Certificados* de entidad final, cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

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

85. En relación con las claves de los *Certificados* de entidad final, cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.6. RENOVACIÓN DEL CERTIFICADO

4.6.1. Circunstancias para la renovación del certificado

86. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.6.2. Quién puede solicitar la renovación del certificado

87. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.6.3. Procesamiento de solicitudes de renovación del certificado

88. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.6.4. Notificación de la renovación del certificado

89. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

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

90. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.6.6. Publicación del certificado renovado

91. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.6.7. Notificación de la renovación del certificado a otras entidades

92. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

4.7.1. Circunstancias para la renovación con regeneración de claves

93. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.7.2. Quién puede solicitar la renovación con regeneración de claves

94. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

95. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.7.4. Notificación de la renovación con regeneración de claves

96. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

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

97. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.7.6. Publicación del certificado renovado

98. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

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

99. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.8. MODIFICACIÓN DEL CERTIFICADO

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

4.8.1. Circunstancias para la modificación del certificado

101. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

102. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

103. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

104. No se estipula la modificación.

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

105. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

106. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

107. No se estipula la modificación.

4.9. REVOCACIÓN DEL CERTIFICADO

108. 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*.

109. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, conllevará automáticamente la extinción de la vigencia de los *Datos de creación de firma* asociados a éste. Dichos efectos surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo hará constar en su *Servicio de información y consulta sobre el estado de los certificados*.

4.9.1. Circunstancias para la revocación

110. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.9.2. Quién puede solicitar la revocación

111. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.9.3. Procedimiento de solicitud de la revocación

112. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.9.4. Periodo de gracia de la solicitud de revocación

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

4.9.5. Plazo de tiempo para procesar la solicitud de revocación

114. La FNMT – RCM procede a la revocación inmediata del certificado en el momento de verificar la identidad del *Titular* o, en su caso, de la veracidad de la solicitud realizada mediante resolución judicial o administrativa.

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

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

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

4.9.7. Frecuencia de generación de CRLs

116. 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 al menos cada 6 meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de 6 meses.

4.9.8. Periodo máximo de latencia de las CRLs

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

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

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

4.9.10. Requisitos de comprobación en línea de la revocación

119. La comprobación en línea del estado de revocación de los *Certificados* AC subordinadas o de entidad final puede realizarse mediante el *Servicio de información del estado de los certificados*, ofrecido a través de OCSP según se describe en el apartado 4.10 "Servicios de información del estado de los certificados" del presente documento. El interesado en utilizar dicho servicio deberá:

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

4.9.11. Otras formas de aviso de revocación disponibles

120. Las definidas en la legislación de aplicación a través de un medio que acredite la entrega y recepción efectiva siempre que sea factible.

4.9.12. Requisitos especiales de revocación de claves comprometidas

121. La FNMT-RCM utilizará medios de comunicación razonables para informar a los *Suscriptores* que su clave privada puede haber sido comprometida. Siempre que se confirme un compromiso de la clave, la FNMT-RCM revocará los *Certificados* afectados conforme a lo descrito en el apartado 4.9 de la presente *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica* y, en su caso, las *Declaraciones de Certificación Particulares* dependientes de esta.

122. La comunicación a la FNMT-RCM sobre el compromiso de una clave privada a través de la cuenta de correo incidentes.ceres@fnmt.es indicada en el apartado 1.5.2, debe incluir en todo caso una prueba de dicho compromiso e indicar en el asunto del correo electrónico: "Compromiso de claves". Para demostrarlo, las partes pueden utilizar los siguientes métodos:

• Envío de la clave privada comprometida o una respuesta de desafío firmada por la clave privada y verificable por la clave pública, así como la propia clave pública.

• Proporcionar referencias a vulnerabilidades y / o fuentes de incidentes de seguridad a partir de las cuales el compromiso de la clave sea verificable.

123. La FNMT-RCM podrá aceptar otro tipo de evidencias que demuestren adecuadamente el compromiso de claves.

4.9.13. Circunstancias para la suspensión

124. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.9.14. Quién puede solicitar la suspensión

125. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.9.15. Procedimiento para la petición de la suspensión

126. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.9.16. Límites sobre el periodo de suspensión

127. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

128. La información sobre el estado de revocación de los *Certificados* permite a los usuarios conocer el estado del *Certificado*, no solo hasta que éste expire, sino más allá de dicha fecha, dado que no se eliminan los certificados revocados de la correspondiente CRL después de que hayan expirado. En caso de cese de la actividad y/o compromiso de claves de la CA, se generará una última CRL que se mantendrá íntegra y disponible para su consulta garantizando la disponibilidad del servicio de información sobre el estado de los certificados, durante al menos 15 años desde su publicación.

129. La provisión de la información sobre el estado de revocación de los *Certificados,* en caso de cese de actividad de la FNMT-RCM como *Prestador de Servicios de Confianza*, queda garantizada mediante la transferencia, a otro Prestador con el que se llegue al correspondiente acuerdo, de toda la información relativa a los *Certificados* y, especialmente, de los datos de su estado de revocación.

130. Cuando la infraestructura realiza la revocación de un *Certificado*, el sistema refleja este hecho en la base de datos consultada por el *Servicio de información y consulta del estado de los Certificados* mediante el protocolo OCSP, al tiempo que genera una nueva CRL y la publica en el repositorio LDAP. La citada base de datos cuenta con una copia de respaldo. En caso de ocurrir algún fallo en la secuencia descrita, se produce una alarma al objeto de subsanar el posible error. De esta forma se garantiza la consistencia de la información suministrada por estos dos métodos (OCSP y consulta de CRL). Adicionalmente se realiza la monitorización periódica del *Directorio* LDAP como mantenimiento preventivo.

131. La información relativa a la verificación del estado de revocación de los *Certificados* electrónicos expedidos por la FNMT-RCM puede ser consultada mediante CRLs y/o el *Servicio de información y consulta del estado de los Certificados* mediante el protocolo OCSP, y son accesibles a través de los siguientes medios:

- Jerarquía AC RAIZ FNMT

  a. Listas de Certificados Revocados:

     1. AC RAIZ “AC RAIZ FNMT-RCM”

        - ldap://ldapfnmt.cert.fnmt.es/CN=CRL,OU=AC%20RAIZ%20FNMT-RCM,O=FNMT-

RCM,C=ES?authorityRevocationList;binary?base?objectclass=cRLDistributionPoint

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

2. AC Subordinada "AC Componentes Informáticos"
   - ldap://ldapcomp.cert.fnmt.es/CN=CRL1,OU=AC%20Componentes%20Informaticos,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
   - http://www.cert.fnmt.es/crlscomp/CRL1.crl
3. AC Subordinada "AC Representación"
   - ldap://ldaprep.cert.fnmt.es/CN=CRL<xxx>,OU=AC%20Representacion,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint
   - http://www.cert.fnmt.es/crlsrep/CRL<xxx*>.crl
4. AC Subordinada "AC FNMT Usuarios"
   - ldap://ldapusu.cert.fnmt.es/CN=CRLU<xxx*>,CN=AC%20FNMT%20Usuarios,OU=CERES,O=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

     *xxx: número entero que identifica la CRL (CRLs particionadas)
   - http://www.cert.fnmt.es/crlsacusu/CRLU<xxx*>.crl
5. AC Subordinada "AC Sector Público"
   - ldap://ldapsp.cert.fnmt.es/CN=CRL<xxx*>,cn=AC%20Sector%20Publico,ou=CERES,o=FNMT-RCM,C=ES?certificateRevocationList;binary?base?objectclass=cRLDistributionPoint

     *xxx: número entero identificador de la CRL (CRLs particionadas)
   - http://www.cert.fnmt.es/crlsacsp/CRL<xxx*>.crl
6. AC Subordinada "AC Unidades de Sellado de Tiempo"
   - http://www.cert.fnmt.es/crlsacst/CRL.crl
7. AC Subordinada "AC Administración Pública" [Caducada]
   - 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=cRL DistributionPoint

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

b. Servicio de comprobación del estado de certificados (OCSP):

1. AC RAIZ "AC RAIZ FNMT-RCM"

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

2. AC Subordinada "AC Componentes Informáticos"

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

3. AC Subordinada "AC Representación"

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

4. AC Subordinada "AC FNMT Usuarios"

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

5. AC Subordinada "AC Sector Público"

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

6. AC Subordinada "AC Unidades de Sellado de Tiempo"

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

7. AC Subordinada "AC Administración Pública" [Caducada]. Servicio no disponible por caducidad de dicha autoridad.

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

- Jerarquía AC RAIZ FNMT G2

a. Listas de Certificados Revocados:

1. AC RAIZ "AC RAIZ FNMT-RCM G2"
   - http://www.cert.fnmt.es/crls/ARLFNMTRCMG2.crl
2. AC Subordinada "AC Consulares G2"
   - http://www.cert.fnmt.es/crlsacconsu/CRL<xxx*>.crl
3. AC Subordinada "AC USUARIOS G2"
   - http://www.cert.fnmt.es/crlacusuG2/CRL<xxx*>.crl
4. AC Subordinada "AC REPRESENTACIÓN G2"
   - http://www.cert.fnmt.es/crlsrepG2/CRL<xxx*>.crl

5. AC Subordinada "AC SECTOR PÚBLICO G2"
   - http://www.cert.fnmt.es/crlsacspG2/CRL<xxx*>.crl
6. AC Subordinada "AC ENTIDADES G2"
   - http://www.cert.fnmt.es/crlacentiG2/CRL<xxx*>.crl

b. Servicio de comprobación del estado de certificados (OCSP):

1. AC RAIZ "AC RAIZ FNMT-RCM G2"
   http://ocspcaraizg2.cert.fnmt.es/ocspcaraizG2/OcspResponder
2. AC Subordinada "AC Consulares G2"
   http://ocspconsug2.cert.fnmt.es/ocspconsuG2/OcspResponder
3. AC Subordinada "AC USUARIOS G2"
   http://ocspusug2.cert.fnmt.es/ocspusuG2/OcspResponder
4. AC Subordinada "AC REPRESENTACIÓN G2"
   http://ocsprepg2.cert.fnmt.es/ocsprepG2/OcspResponder
5. AC Subordinada "AC SECTOR PÚBLICO G2"
   http://ocspspg2.cert.fnmt.es/ocspspG2/OcspResponder
6. AC Subordinada "AC ENTIDADES G2"
   http://ocspentig2.cert.fnmt.es/ocspentiG2/OcspResponder

- Jerarquía AC RAIZ FNMT TSA

a. Listas de Certificados Revocados:

1. AC RAIZ "AC RAIZ FNMT-RCM TSA"
   - http://www.cert.fnmt.es/crls/ACRAIZFNMTTSA.crl
2. AC Subordinada "AC TSA FNMT"
   - http://www.cert.fnmt.es/crlsactsafnmtg2/CRL.crl
3. AC Subordinada "AC TSA CLIENTES"
   - http://www.cert.fnmt.es/crlsactsafnmtclig2/CRL.crl

b. Servicio de comprobación del estado de certificados (OCSP):

1. AC RAIZ "AC RAIZ FNMT-RCM TSA"
   http://ocspraiztsa.cert.fnmt.es/ocspraiztsa/OcspResponder

2. AC Subordinada "AC TSA FNMT"

   http://ocsptsag2.cer.fnmt.es/ocsptsaG2/OcspResponder

3. AC Subordinada "AC TSA CLIENTES"

   http://ocsptsaclig2.cert.fnmt.es/ocsptsacliG2/OcspResponder

4.10.1. Características operativas

132. El funcionamiento del *Servicio de información y consulta del estado de los Certificados* es el siguiente: el servidor OCSP de la FNMT-RCM recibe la petición OCSP efectuada por un Cliente OCSP y comprueba el estado de los *Certificados* incluidos en la misma. En caso de que la petición sea válida, se emitirá una respuesta de OCSP informando acerca del estado en el que se encuentran en ese momento los *Certificados* incluidos en la petición. Dicha respuesta OCSP está firmada con los *Datos de Creación de Firma* / *Sello* asociados al servidor OCSP específico para cada AC, garantizando así la integridad y la autenticidad de la información suministrada sobre el estado de revocación de los *Certificados* consultados.

133. El *Servicio de información y consulta del estado de los Certificados* mediante protocolo OCSP soporta el método GET para recuperar la información de validación de los certificados emitidos, de acuerdo con los requisitos de la RFC6960 y aquellos establecidos por la entidad CA/Browser Forum (que pueden consultarse en la dirección https://cabforum.org/). Las respuestas OCSP tienen un intervalo de validez de 8 horas y la información se actualiza constantemente accediendo directamente a la base de datos de cada CA. El *OCSP Responder* no responderá *"good"* a la consulta sobre el estado de un certificado que no ha sido emitido.

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

4.10.2. Disponibilidad del servicio

135. La FNMT-RCM garantiza el acceso a este servicio, en horario 24x7, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento. La FNMT-RCM notificará esta última circunstancia en la dirección http://www.ceres.fnmt.es si es posible con al menos cuarenta y ocho (48) horas de antelación y tratará de solventarla en un periodo no superior a veinticuatro (24) horas. El servicio será accesible para todos los *Usuarios*, *Titulares* y las partes que confían en los *Certificados*, de forma segura, rápida y gratuita.

4.10.3. Características opcionales

136. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

137. La suscripción finalizará en el momento en el que quede sin efecto el *Certificado*. De no llevarse a cabo la renovación del *Certificado* se considerará extinguida la relación entre el *Suscriptor* y la FNMT-RCM.

138. Los *Certificados* emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

a) Terminación del período de validez del *Certificado.*

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, una vez acreditada la ausencia de oposición de los *Suscriptores*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

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

c) Revocación del *Certificado* por cualquiera de las causas recogidas en la correspondiente *Declaración de Prácticas de Certificación*.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

139. La FNMT-RCM no recuperará las *Claves privadas* de los *Titulares* de los *Certificados*.

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

140. No estipulado.

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

141. La FNMT, como *Prestador de Servicios de Confianza*, mantiene todos los sistemas que son críticos en una o más zonas seguras, tanto física como funcional y lógicamente.

142. Así mismo, cuenta con redes dedicadas y separadas para la administración de sus sistemas informáticos y para la operación de los servicios de confianza. Los sistemas utilizados para la administración de la implementación de la política de seguridad no se utilizan para otros fines. Los sistemas de producción para los servicios de confianza están separados de los sistemas utilizados en desarrollo y prueba.

143. 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 confianza. 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.

144. A continuación y tomando como modelo de trabajo el documento *RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, y los estándares europeos *ETSI* EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 411 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates" y ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" y los requisitos CAB Forum "Network and Certificate System Security Requirements", se muestran todos los controles implementados por la FNMT-RCM como *Prestador de Servicios de Confianza*, sin perjuicio de los de carácter confidencial y secreto de los que no se informa por razones de seguridad.

5.1. CONTROLES DE SEGURIDAD FÍSICA

145. 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.

146. 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.

5.1.1. Ubicación de las instalaciones

147. El edificio donde se encuentra ubicada la infraestructura del *Prestador de Servicios de Confianza*, 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.

5.1.1.1. Situación del Centro de Proceso de Datos

148. El CPD del *Prestador de Servicios de Confianza* 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 confianza se encuentran en el entorno de alta seguridad, separado del resto de actividades de la Entidad.

5.1.2. Acceso Físico

5.1.2.1. Perímetro de seguridad física

149. Una vez marcadas las áreas de seguridad donde se desarrolla la actividad FNMT-RCM como *Prestador de Servicios de Confianza* , 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.

150. 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 intrusión, detectores de incendios, etc., además de los medios humanos dedicados a su atención tanto en el exterior como en el interior del recinto.

5.1.2.2. Controles físicos de entrada

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

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

153. 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.

5.1.2.3. El trabajo en áreas seguras

154. 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.

5.1.2.4. Visitas

155. 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.

5.1.2.5. Áreas aisladas de carga y descarga

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

5.1.3. Electricidad y Aire Acondicionado

157. Las salas donde se ubican las máquinas de la infraestructura del *Prestador de Servicios de Confianza*, 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.

158. 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 Confianza*.

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

5.1.3.1. Seguridad del cableado

160. 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.

5.1.4. Exposición al agua

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

5.1.5. Prevención y Protección contra incendios

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

5.1.6. Almacenamiento de Soportes

163. La FNMT-RCM, como *Prestador de Servicios de Confianza*, establece los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva. Todos los soportes son gestionados de forma segura de acuerdo con los requisitos del esquema de clasificación de la información, según lo descrito por la Norma de "Clasificación y control de los recursos de la información" que desarrolla la Política de Seguridad de la Información de la FNMT-RCM. Los soportes que contienen datos confidenciales son desechados de manera segura cuando ya no son necesarios.

5.1.6.1. Recuperación de la información

164. 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.

5.1.7. Eliminación de Residuos

165. 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.

5.1.8. Copias de Seguridad fuera de las instalaciones

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

5.2. CONTROLES DE PROCEDIMIENTO

167. La FNMT-RCM cuenta con una Política de Seguridad de la Información, aprobada por su Director General, ratificada por parte del Comité de Seguridad de la Información y del Comité de Dirección, y está sometida a un proceso de revisión periódica y actualización permanente para garantizar su adecuación a las necesidades de la organización, a la legislación vigente y a los continuos avances tecnológicos. El intervalo máximo entre dos revisiones de la Política de Seguridad de la Información es de un año. La participación de un miembro del Comité de Gestión del PSC en el Comité de Seguridad de la Información garantiza la adecuación de la prestación de los servicios de confianza a dicha Política y la participación en el citado proceso de actualización de la misma.

168. 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 8 "Auditorías de cumplimiento").

- 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.

169. 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.

170. 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.

171. 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.

172. 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. Adicionalmente, la normativa[1] específica que aplica a los roles de confianza, como personal al servicio de la Administración, garantiza la imparcialidad de las operaciones en la actividad de la FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza*.

5.2.1. Roles de confianza

173. 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.

[1] Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

5.2.2. Número de personas por tarea

174. Las tareas asignadas a las personas, según el rol de confianza desempeñado, quedan recogidas en el documento interno de la Dirección de Sistemas de Información de la FNMT – RCM definido como "Roles de Confianza y perfiles de seguridad".

5.2.3. Identificación y autenticación para cada rol

175. 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".

5.2.4. Roles que requieren segregación de funciones

176. Los Roles de Confianza definidos son: Oficial de Seguridad, Administrador del Sistema, Operador del Sistema, Auditor del Sistema y Especialista de Validación. La selección de las personas a las que se asignan estos roles se realiza conforme al principio de "privilegio mínimo" y teniendo en cuenta su formación, experiencia y los controles de Seguridad de Personal descritos a continuación. Las personas que ejercerán estos roles serán designadas por el Comité de Gestión del PSC.

5.3. CONTROLES DE PERSONAL

177. 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 Confianza, 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.

178. 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. Por tanto, la FNMT-RCM administra el acceso de los operadores, administradores y auditores del sistema, con suficientes controles de seguridad lógica para garantizar la separación de roles de confianza identificados en las prácticas de sus servicios de confianza, de forma que los privilegios relacionados con el acceso a aplicaciones críticas de la infraestructura del *Prestador de Servicios de Confianza* cuentan con un tratamiento especial, identificando y autenticando previamente al personal con dicho acceso y dotándole de certificados electrónicos en tarjetas criptográficas.

179. 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.

180. 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.

181. 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.

182. 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.

183. 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.

184. 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.

185. 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.

186. 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.

5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos

187. Todo el personal involucrado en la actividad de la FNMT-RCM, como *Prestador de Servicios de Confianza*, y especialmente el personal directivo, poseen la experiencia y los conocimientos necesarios para gestionar dicha actividad. Estos requisitos quedan garantizados mediante la aplicación de los correspondientes criterios en los procesos de selección de personal para que el perfil profesional del empleado sea el más adecuado posible a las características propias de las tareas a desarrollar.

188. 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.

189. 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* y la información sobre del estado de los *Certificados.*

5.3.2. Procedimientos de verificación de antecedentes

190. 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.

5.3.3. Requisitos de formación

191. 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”.

192. Para el personal que realiza tareas de verificación de información, la formación anual cubrirá conocimientos básicos de Infraestructura de clave pública, políticas, normativa y procedimientos de autenticación y verificación (incluida la Política de certificados y / o Declaración de prácticas de certificación de la FNMT), además de amenazas comunes al proceso de verificación de información (incluido el phishing y otras tácticas de ingeniería social).

193. La FNMT-RCM conserva registros de dicha formación y asegura que el personal encargado de las funciones de Especialista en Validación mantenga las habilidades y conocimientos que le permita desempeñar dichas funciones de manera satisfactoria.

194. La FNMT-RCM documenta que cada Especialista en Validación posee las habilidades y conocimientos requeridos por una tarea, antes de permitirle realizarla.

195. La FNMT-RCM requiere que todos los Especialistas en Validación superen un examen sobre los requisitos de verificación de información.

5.3.4. Requisitos y frecuencia de actualización formativa

196. La FNMT-RCM lleva a cabo planes de formación continua, con especial interés en los casos de modificaciones sustanciales en la operativa de la infraestructura dedicada a la prestación de los *Servicios de Confianza*.

5.3.5. Secuencia y frecuencia de rotación laboral

197. No estipulado.

5.3.6. Sanciones por acciones no autorizadas

198. 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.

199. 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.

...”

200. 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.

201. 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.

5.3.7. Requisitos de contratación de personal

202. 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 51/2023, de 31 de enero, por el que se aprueba el Estatuto de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, Entidad Pública Empresarial, Medio Propio).

203. 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.

5.3.7.1. Requisitos de contratación de terceros

204. Las contrataciones de terceros realizadas por la FNMT – RCM están sometidas a la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (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.

5.3.8. Suministro de documentación al personal

205. 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.

206. 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.

207. 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.

208. 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.

5.4. PROCEDIMIENTOS DE AUDITORÍA

209. 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.

210. 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.

5.4.1. Tipos de eventos registrados

211. 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. Dichos eventos registrados se pondrán a disposición, si es necesario, con el fin de proporcionar pruebas del correcto funcionamiento de los servicios a efectos de procedimientos judiciales.

212. Los eventos registrados serán todas aquellas operaciones que se realicen en la gestión de claves, gestión de *Certificados*, emisión de *Sellos de Tiempo electrónicos*, información sobre el estado de *Certificados*, publicación, archivo, recuperación, directorio, registro de eventos y registro de usuarios. Serán registrados todos los eventos relacionados con el ciclo de vida de las claves administradas por la AC y, en su caso, las generadas por esta. También formarán parte de los eventos registrados la información relativa a los procesos de registro (acreditación de la identidad), como los datos únicos de identificación, acuerdo firmado por el Solicitante, Entidad a la que pertenece la Oficina de Registro, etc., según se especifica en los correspondientes documentos de Procedimientos de Registro.

213. FNMT-RCM guardará registro de al menos los siguientes eventos:

a) Certificados de CA y eventos de ciclo de vida de claves, incluyendo:

1. Generación de claves, backup, almacenamiento, recuperación, archivo, y destrucción;
2. Solicitudes, renovaciones, solicitudes con renovación de claves, y revocaciones de certificados;

3. Aprobación y rechazo de solicitudes de certificados;
4. Eventos de la gestión del ciclo de vida de los dispositivos criptográficos;
5. Generación de entradas en las CRLs y OCSP;
6. Actualización de los perfiles de los certificados.

b) Eventos de la gestión del ciclo de vida de los certificados de los Suscriptores, incluyendo:

1. Solicitudes de certificados, solicitudes de renovación y renovación de claves y revocación;
2. Todas las actividades de verificación estipuladas en esta DPC;
3. Aprobación y rechazo de las solicitudes de certificados;
4. Emisión de certificados; y
5. Generación de entradas en las CRLs y OCSP.

c) Eventos de seguridad, incluyendo:

1. Intentos de acceso al sistema PKI exitosos y fallidos;
2. Acciones realizadas en la PKI y sistemas de seguridad;
3. Cambios en los perfiles de seguridad;
4. Instalación, actualización y borrado de software en el sistema de generación de certificados;
5. Caídas del sistema, fallos de hardware, y otras anomalías;
6. Actividades con Firewall y enrutadores (ver sección 5.4.1.1); y
7. Entradas y salidas de las instalaciones de la CA

214. La FNMT-RCM mantendrá archivados todos los eventos registrados más importantes, manteniendo su accesibilidad, durante un periodo nunca inferior a 15 años.

215. Todos los eventos registrados son susceptibles de auditarse e incluirán la fecha y hora del registro, la identidad de la persona que lleva a cabo el registro del diario, así como una descripción del registro.

216. La FNMT-RCM pondrá a disposición de las autoridades competentes las evidencias relativas a los eventos registrados que obren en su poder, mediante requerimiento judicial o el correspondiente procedimiento legal, previa solicitud por escrito realizada a los datos de contacto descritos en el apartado “1.5.2. Datos de contacto”.

217. Adicionalmente a los eventos expuestos, se guardarán todos los registros que especifica la norma ISO 9001 y SR10 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

5.4.1.1. Registro o Log de actividades con Firewall y enrutadores

218. El registro de las actividades del Firewall y los routers (enrutadores) incluye:

1. Intentos de registro exitosos y fallidos a los routers y firewalls, y
2. Registro de todas las acciones administrativas realizadas en los routers y en los firewalls, incluyendo cambios de configuraciones, actualizaciones de firmware y modificaciones en el control de acceso, y
3. Registro de todos los cambios en las reglas del Firewall, incluyendo añadidos, modificaciones y borrados, y
4. Registro de todos los eventos del sistema y errores, incluyendo fallos de hardware, cuelgues de software y reinicios del sistema.

5.4.2. Frecuencia de procesamiento de registros

219. Los registros son analizados de forma continua, si bien serán auditados de manera manual cuando sea necesario. Por ejemplo, en caso de que se produzca una alerta del sistema motivada por la existencia de algún incidente, no existiendo una frecuencia definida para dicho proceso.

5.4.3. Periodo de conservación de los registros

220. La FNMT conservará los registros de auditoria por al menos quince (15) años:

1. Los certificados de la CA y los eventos de la gestión del ciclo de vida de las claves como se establece en la sección 5.4.1 después de la última ocurrencia de:
   a. la destrucción de la clave privada de la CA; o
   b. la revocación o caducidad del certificado de la CA del conjunto de certificados que tienen la extensión X.509v3 basicConstraints con el campo CA establecido en “true” y que comparten una clave pública común, correspondiente a la clave privada de la CA;
2. Eventos de la gestión del ciclo de vida de los certificados de los Suscriptores como se establece en la sección 5.4.1 después de la revocación o caducidad del certificado;
3. Cualquier evento de seguridad como se establece en la sección 5.4.1 después de que se produzca

5.4.4. Protección de los registros

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

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

223. 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.

224. 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.

5.4.5. Procedimientos de copias de seguridad de los registros auditados

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

5.4.6. Sistema de recolección de registros

226. Los eventos significativos generados por las ACs y por las ARs son convenientemente almacenados en los sistemas internos de la FNMT-RCM.

5.4.7. Notificación al sujeto causante de los eventos

227. No se contempla.

5.4.8. Análisis de vulnerabilidades

228. La FNMT-RCM realiza trimestralmente un análisis de vulnerabilidades en sus sistemas. Adicionalmente se realiza un test anual de penetración.

5.5. ARCHIVADO DE REGISTROS

5.5.1. Tipos de registros archivados

229. La FNMT-RCM archivará y mantendrán accesible toda la información pertinente referente a los datos expedidos y recibidos, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad de sus Servicios de Confianza.

230. 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 Confianza*.
- 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 al *Servicio de información sobre el estado de los certificados*.
- Eventos relevantes de la generación de pares de números aleatorios y seudoaleatorios 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.

231. Además de dichos eventos, se archiva también toda la documentación relacionada, por ejemplo:

- Documentación relativa a los protocolos de generación y conservación de las Claves de las Autoridades de Certificación y del Servicio de Sellado de tiempo.
- Solicitudes de emisión y revocación de Certificados,
- Documentación relativa a las operaciones de acreditación realizadas por las oficinas de registro.
- Eventos relacionados con la prestación del servicio de firma en servidor
- Declaraciones de Prácticas y Políticas de Certificación y su histórico.

5.5.2. Periodo de retención del archivo

232. El periodo de retención de los registros archivados no será inferior a 15 años tras la extinción de la vigencia del certificado asociado o finalización del servicio prestado.

5.5.3. Protección del archivo

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

234. 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 *Acuerdos* correspondientes.

235. 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.

5.5.4. Procedimientos de copia de respaldo del archivo

236. En todo momento existirá una copia de seguridad de todos los archivos considerados críticos para la realización de la actividad de la FNMT-RCM como *Prestador de Servicios de Confianza*.

5.5.5. Requisitos para el sellado de tiempo de los registros

237. 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".

5.5.6. Sistema de archivo

238. 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.

239. 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.

5.5.7. Procedimientos para obtener y verificar la información archivada

240. Estos sistemas de archivos están provistos de un alto nivel de integridad, confidencialidad y disponibilidad para evitar intentos de manipulación de los certificados y eventos almacenados.

5.6. CAMBIO DE CLAVES DE LA AC

241. Con anterioridad a la expiración del periodo de vigencia del certificado de una *Autoridad de Certificación* raíz, o de una *Autoridad de Certificación* subordinada, se procederá a la creación de una 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.

5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

5.7.1. Gestión de incidentes y vulnerabilidades

242. 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.

243. 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. Adicionalmente, se realizan auditorías periódicas de los procedimientos emprendidos y se monitoriza y evalúa periódicamente la gestión de vulnerabilidades técnicas.

244. La FNMT-RCM abordará cualquier vulnerabilidad crítica no prevista en un período de 48 horas después de su descubrimiento. Una vez analizado su impacto la vulnerabilidad crítica será documentada y se decidirá sobre su resolución mediante un plan de mitigación de la misma, en función del coste de su resolución.

245. 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. Si se produjera algún incidente de alto impacto, la FNMT-RCM lo notificará en menos de 24 horas desde la detección del mismo.

5.7.2. Actuación ante datos y software corruptos

246. Esta contingencia está contemplada en el Plan de continuidad de negocio de la FNMT – RCM.

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

247. 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 informar de los hechos a las partes afectadas y a los navegadores en cuyos programas raíces estén incluidos los certificados de la FNMT-RCM.
4) Estudiar la necesidad de ejecutar el Plan de Cese de Actividades del PSC según la DPC y legislación vigente.

5.7.4. Continuidad de negocio después de un desastre

248. La FNMT-RCM cuenta con un Plan de continuidad de negocio que describe las actuaciones a llevar a cabo en casos de desastre. Para ello, cuenta con un sistema de copia de seguridad que almacena de forma segura los datos necesarios para reanudar las operaciones de las Autoridades de Certificación en caso de incidentes, incluso en el centro de respaldo alternativo, con el objetivo de garantizar que toda la información esencial y el software puedan recuperarse después de un desastre o un fallo de los medios.

249. Para garantizar la continuidad del negocio después de una contingencia o desastre, los medios de respaldo son probados regularmente mediante simulacros, al menos una vez al año, siguiendo lo establecido en el Plan de Pruebas del Plan de continuidad de negocio de la FNMT-RCM.

250. En el caso de fallo o desastre de los sistemas del *Prestador de Servicios de Confianza,* se 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 Confianza* o compromiso de los algoritmos criptográficos que supongan una amenaza real, considerando el estado actual de la técnica, de suplantación de la identidad. En estos casos la FNMT-RCM procederá a planificar la revocación de los *Certificados* afectados e informará a todos los miembros de la Comunidad Electrónica indicando que todos los *Certificados*, *Listas de Revocación*, *Sellos de tiempo electrónicos* 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.

251. 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.

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

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

253. 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 Confianza* 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
- Podrá transferir, una vez acreditada la ausencia de oposición de los *Suscriptores*, aquellos *Certificados* que sigan siendo válidos en la fecha efectiva de cese de actividad a otro *Prestador de Servicios de Confianza* 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 *Organismo de supervisión* 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.

254. 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.

255. En el caso de que el cese está relacionado con el *Servicio de firma remota*, la FNMT-RCM:

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

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES

6.1.1. Generación del par de Claves

6.1.1.1. Generación del par de Claves de la CA

256. La FNMT-RCM cuenta con un procedimiento, descrito en el documento interno "Gestión del ciclo de vida de las claves de la FNMT-RCM como Prestador de Servicios de Certificación y Sellado", para llevar a cabo la generación del par de claves de AC para todas sus *Autoridades de Certificación*, tanto raíces como subordinadas que emiten *certificados* a los *usuarios* finales. Como resultado de dicho procedimiento, se elabora un informe que demuestra que la ceremonia correspondiente se ha llevado a cabo de conformidad con el procedimiento establecido, y que se garantizan la integridad y la confidencialidad del par de claves. Dicho informe es firmado por las personas que ejercen los correspondientes roles de confianza en la generación de Claves de una AC subordinada, y en el caso de una AC raíz será firmado adicionalmente por auditor confiable e independiente del equipo de gestión del *Prestador*. El citado procedimiento describe los siguientes puntos:

- los roles que participan en la ceremonia de claves;
- las funciones que realiza cada rol y en qué fases;
- responsabilidades durante y después de la ceremonia; y
- los requisitos de evidencia que se recopilan de la ceremonia.

257. El procedimiento para la emisión, firma y distribución de nuevos *Certificados* de AC especifica que, antes de la expiración del *Certificado,* se genera uno nuevo, evitando así posibles interrupciones en las operaciones de cualquier entidad que pueda confiar en el *Certificado*.

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

259. 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, 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 aplicables a los *Prestadores de servicios de confianza*.

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

261. 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*.

6.1.1.2. Generación del par de Claves de la RA

262. No estipulado.

6.1.1.3. Generación del par de Claves de los Suscriptores

263. Las *Claves privadas* de los *Titulares* de los *Certificados* son generadas y custodiadas según se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de Confianza*.

6.1.2. Envío de la clave privada al suscriptor

264. El envío de las *Claves privadas* de los *Titulares* de los *Certificados,* se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de Confianza.*

6.1.3. Envío de la clave pública al emisor del certificado

265. El envío de las *Claves públicas* de los *Titulares* de los *Certificados* al emisor, se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de Confianza*.

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

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

267. 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 1.3.1. Autoridad de Certificación).

6.1.5. Tamaños de claves y algoritmos utilizados

268. El algoritmo utilizado es sha256WithRSAEncryption or sha384WithRSAEncryption para la jerarquía dependiente del certificado AC RAÍZ FNMT-RCM y ecdsa-with-SHA384 o ecdsa-with-SHA256 para la jerarquía dependiente del certificado AC RAÍZ FNMT-RCM G2 y AC RAÍZ FNMT-RCM TSA.

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

- Claves de la AC RAÍZ FNMT-RCM: 4.096 bits.
- Claves de la AC RAÍZ FNMT-RCM G2: 384 bits (ECC P-384).
- Claves de la AC RAÍZ FNMT-RCM TSA: 384 bits (ECC P-384).

- Claves de las ACs FNMT Subordinadas que expide los Certificados de entidad final: se describe en cada Declaración de Políticas de Certificación y Prácticas de Certificación Particulares definida para cada Servicio de Confianza.
- Claves de los Certificados de entidad final: se describe en cada Declaración de Políticas de Certificación y Prácticas de Certificación Particulares definida para cada Servicio de Confianza.

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

270. Las *Claves públicas* de los *Certificados* están codificadas de acuerdo con RFC5280 y PKCS#1.

271. Se emplean los parámetros recomendados en el documento de especificaciones técnicas ETSI TS 119 312, "Electronic Signatures and Infraestructures (ESI); Cryptographic Suites".

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

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

273. Los *Certificados* de las ACs FNMT Raíces que expiden los Certificado de las ACs FNMT Subordinadas tienen habilitados exclusivamente los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.

274. Los *Certificados* de las ACs FNMT Subordinadas que expiden los *Certificados* de entidad final tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de usuario final y CRLs.

275. Los usos de las *Claves* de los *Certificados* de entidad final, se describen en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de Confianza*.

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

6.2.1. Estándares para los módulos criptográficos

276. Los *Datos de creación de firma* del *Prestador de Servicios de Confianza* 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 electrónicos* son llevadas a cabo dentro del dispositivo criptográfico, que dota de *Confidencialidad* a los *Datos de creación de Firma* del *Prestador de Servicios de Confianza*.

277. 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*.

278. Los *Dispositivos de cualificados de creación de firma* (QSCD) utilizados por la FNMT-RCM, cumplen con los estándares Common Criteria (CC) Information Technology Evaluation Assurance Level (EAL) EAL 4+ o equivalente.

279. La FNMT-RCM revisará el estado de la certificación de los *Dispositivos cualificados de creación de firma* para verificar que continúan cumpliendo con los requisitos establecidos por el reglamento eIDAS. En el caso de que dichos dispositivos perdieran la certificación como QCSD, los *Certificados* activos en los que *Claves privadas* se encuentren en el QSCD afectado serán revocados.

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

280. Los mecanismos de activación y uso de las *Claves privadas* de sus *Autoridades 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 n de m (2 de 5).

6.2.3. Custodia de la clave privada

281. 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.

282. Las *Claves Privadas* de los *Titulares* son mantenidas, con un alto nivel de confianza, bajo el control exclusivo del propio *Titular*. En caso de *Certificados de Firma Centralizada* la *Clave Privada* (*Datos de creación de firma*) estará custodiada por el Prestador de Servicios de Confianza en nombre de su *Titular*, de conformidad con la legislación aplicable. Cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los Certificados expedidos bajo dichas políticas.

6.2.4. Copia de seguridad de la clave privada

283. 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.

6.2.5. Archivado de la clave privada

284. La FNMT-RCM podrá efectuar una copia de seguridad de las *Claves Privadas,* garantizando que el grado de seguridad de los datos duplicados es del mismo nivel que el de los datos originales y que el número de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio. No se duplican los *Datos de creación de firma* para ninguna otra finalidad. No obstante, cada Declaración de Políticas de Certificación Particulares determinará este aspecto para los *Certificados* expedidos bajo dichas políticas.

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

285. La generación de las *Claves Privadas* de las *Autoridades de Certificación* se realiza según lo descrito en el apartado "6.1 Generación e instalación de las *Claves*". Por tanto, no es posible la transferencia dichas *Claves*, si bien existe un procedimiento de recuperación de las mismas como medida de contingencia, como se describe en el apartado "6.2.4 Copia de seguridad de la clave privada".

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

286. 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 Confianza:*

- 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.

287. Las *Claves Privadas* de las AC raíz se mantienen y utilizan físicamente aisladas de las operaciones normales, de modo que solo el personal de confianza designado tiene acceso a dichas claves para utilizarlas en la firma/sello de *Certificados* de AC subordinadas.

6.2.8. Método de activación de la clave privada

288. 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.

289. Los mecanismos de activación y uso de las *Claves Privadas* de los *Certificados* de entidad final, se describen en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de confianza.*

6.2.9. Método de desactivación de la clave privada

290. Una persona con el rol de administrador, puede proceder a la desactivación de la clave de las *Autoridades de Certificación* mediante la detención del sistema. Para su reactivación se actuará según lo descrito en el apartado "6.2.8 Método de activación de la clave privada".

291. En cuanto a la desactivación de las *Claves Privadas* de los *Certificados* de entidad final, se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de confianza.*

6.2.10. Método de destrucción de la clave privada

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

293. En el caso de las *Claves Privadas* de los *Certificados* de entidad final, este método se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de Confianza.*

6.2.11. Clasificación de los módulos criptográficos

294. Los módulos criptográficos cumplen con los requisitos de seguridad necesarios para garantizar la protección de las *Claves*, según lo indicado en el apartado "6.2.1 Estándares para los módulos criptográficos" del presente documento.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. Archivo de la clave pública

295. La FNMT-RCM conservará la *Clave Pública* del *Titular* y la prueba de posesión de la *Clave Privada* (*Clave Pública* cifrada con la *Clave Privada*) según el ordenamiento legal vigente, durante un periodo no menor a 15 años tras la extinción de la vigencia del certificado asociado.

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

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

- *Certificado* de la AC raíz FNMT-RCM y su par de *Claves*: hasta el 1 de enero de 2030.
- *Certificado* de la AC raíz FNMT-RCM G2 y su par de *Claves*: hasta el 4 de octubre de 2049.
- *Certificado* de la AC raíz FNMT-RCM TSA y su par de *Claves*: hasta el 4 de octubre de 2049.
- Los *Certificados* de la ACs subordinadas que expiden los *Certificados* de entidad final: se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de confianza.*
- Los *Certificados* de entidad final*:* se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de confianza.*

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

297. Los datos de activación, tanto de las *Claves* de las ACs FNMT raíz como de las *Claves* de las ACs subordinadas que expiden los *Certificados* de entidad final, se generan durante la ceremonia de *Claves* de creación de dichas *Autoridades de Certificación*.

298. En cuanto a los datos de activación de las *Claves* de los *Certificados* de entidad final, se describen, en su caso, en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de confianza.*

6.4.2. Protección de datos de activación

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

6.4.3. Otros aspectos de los datos de activación

300. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1. Requisitos técnicos específicos de seguridad informática

301. 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 Confianza*, 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 Confianza*, así como la normativa EESSI.

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

6.5.1.1. Comunicación de las incidencias de seguridad

303. 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, 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".

6.5.1.2. Comunicación de las debilidades de seguridad

304. 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.

6.5.1.3. Comunicación de los fallos del software

305. Los fallos del software son clasificados como incidencias y, como tales, se resuelven dando lugar a las oportunas acciones correctivas, según se describe en los procedimientos anteriormente mencionados.

6.5.1.4. Aprendiendo de las incidencias

306. 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.

6.5.2. Evaluación del nivel de seguridad informática

307. 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.

308. 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 Confianza*, 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.

309. 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", normativa bajo la cual la FNMT-RCM cuenta con la correspondiente certificación en el ámbito de los sistemas implicados en la Prestación de servicios de confianza.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

6.6.1. Controles de desarrollo de sistemas

310. Antes de abordar un proyecto de desarrollo de software, el *Prestador de Servicios de Confianza* 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 sometidos a un proceso de valoración de riesgos y análisis de requisitos de seguridad.

311. El proceso de evolución de las aplicaciones informáticas del *Prestador de Servicios de Confianza* 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.

6.6.2. Controles de gestión de la seguridad

312. La integridad de la información y los sistemas de la FNMT-RCM, como *Prestador de Servicios de Confianza,* es protegida contra virus, software malicioso y no autorizado.

313. La FNMT-RCM cuenta con procedimientos que garantizan la aplicación de los parches de seguridad en el mínimo tiempo posible desde su disponibilidad, salvo que su aplicación introduzca vulnerabilidades o fallos de funcionamiento, en cuyo caso se documentarán las razones de su no aplicación.

6.6.3. Controles de seguridad del ciclo de vida

314. La FNMT-RCM aplica controles de seguridad durante todo el ciclo de vida de los sistemas, entre los que se incluye la gestión de soportes, frente a la obsolescencia y el deterioro de los medios de almacenamiento, durante el periodo de tiempo requerido, de conformidad con lo establecido en el documento interno de "Backup y Políticas de Restauración y Arquitectura".

6.6.3.1. Actualización de algoritmia

315. 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.

6.7. CONTROLES DE SEGURIDAD DE LA RED

316. La FNMT-RCM segmenta sus sistemas en redes o zonas teniendo en cuenta la relación funcional, lógica y física entre los sistemas y servicios confiables.

317. Para la correcta *Prestación de los servicios de confianza* se requiere acceso externo a los mismos a través de Internet y/u otras redes (por ejemplo, Red SARA). El acceso a Internet en el Centro de Datos Principal está redundado y, adicionalmente, el acceso a Internet del Centro de Respaldo es proporcionado por un operador diferente. Los mecanismos de conmutación de operadores son automáticos. El acceso a Red SARA también está redundado en el Centro de Datos Principal y existe un backup en el Centro de Respaldo, de forma que, en caso de

necesidad, se activa desde el Centro de Operaciones de Red SARA bajo petición de FNMT-RCM.

318. 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.

319. 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.

320. La FNMT-RCM somete su sistema a un análisis periódico de vulnerabilidades en direcciones IP públicas y privadas identificadas como PSC. El Área de Seguridad y Normalización de la FNMT-RCM monitoriza los controles establecidos en el citado plan de acción.

321. La FNMT-RCM somete a una prueba de penetración los sistemas relacionados con la provisión de *Servicios de Confianza*, de forma previa a su puesta en producción y después de las actualizaciones o modificaciones de infraestructura o aplicación consideradas significativas. Las pruebas de penetración y la gestión de los resultados son responsabilidad del Área de Seguridad y Normalización de la FNMT-RCM, que garantiza su ejecución por personal independiente, que dispone de las habilidades, herramientas, competencia, código de ética e independencia necesarios para proporcionar un informe confiable.

322. La FNMT-RCM cuenta con un procedimiento para llevar a cabo las tareas relacionadas con el análisis periódico de vulnerabilidades y con la prueba anual de penetración, tratando los resultados de los mismos, en cuanto a su valoración, elaboración posterior del correspondiente plan de acción para la corrección y, en su caso, para su correspondiente asunción de riesgos.

6.8. FUENTE DE TIEMPO

323. La FNMT-RCM utiliza, como fuente de tiempo, una conexión con el Real Observatorio de la Armada (referencia temporal UTC), en virtud del acuerdo establecido entre ambas Instituciones para la sincronización temporal de sus sistemas. El Real Observatorio de la Armada (ROA) ostenta el patrón de tiempo oficial en España.

6.9. OTROS CONTROLES ADICIONALES

6.9.1. Control de la capacidad de prestación de los servicios

324. La FNMT-RCM realiza controles periódicos del grado de demanda de los servicios relacionados con su actividad como *Prestador de Servicios de Confianza* 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.

6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas

325. Antes de abordar cualquier nuevo proyecto de desarrollo de software, o en caso de requerirse un cambio en algún desarrollo existente, se valorará el establecimiento de controles adicionales a los especificados en los procedimientos en vigor.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

326. 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 Confianza*.

7.1.1. Número de versión

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

7.1.2. Extensiones del certificado

328. En el anexo del presente documento se incluyen los perfiles completos de los *Certificados* de la AC RAIZ FNMT-RCM, de la AC RAIZ FNMT-RCM G2 y de la AC RAIZ FNMT-RCM TSA.

329. En la página http://www.cert.fnmt.es/dpcs/ se publican documentos que describen los perfiles de los *Certificados* expedidos por la FNMT-RCM, incluyendo todas sus extensiones.

7.1.3. Identificadores de objeto de algoritmos

330. El identificador de objeto (OID) correspondiente al algoritmo criptográfico utilizado para:

- la AC RAIZ FNMT-RCM (SHA-256 with RSA Encryption) es 1.2.840.113549.1.1.11.
- la AC RAIZ FNMT-RCM G2 (ecdsa-with-SHA384) es 1.2.840.10045.4.3.3.
- la AC RAIZ FNMT-RCM TSA (ecdsa-with-SHA384) es 1.2.840.10045.4.3.3.

7.1.4. Formatos de nombres

331. La codificación de los *Certificados* sigue la recomendación RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. Todos los

campos definidos en el perfil de estos *Certificados,* excepto en los campos que específicamente se exprese lo contrario, emplean la codificación UTF8String.

332. Los *Certificados* no deben contener metadatos como ".", "-" y "" (es decir, espacio) o cualquier indicación de que un valor o campo está ausente, incompleto o no sea de aplicación.

7.1.5. Restricciones de nombres

333. El nombre distintivo (*DN*) asignado al *Suscriptor* del *Certificado* dentro del dominio del *Prestador de Servicios de Confianza* será único y con la composición definida en el perfil del *Certificado*.

7.1.6. Identificador de objeto de política de certificado

334. El identificador de objeto (OID) de la política de los *Certificados* expedidos por la FNMT-RCM, se describe en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* definida para cada *Servicio de Confianza*.

7.1.7. Empleo de la extensión restricciones de política

335. La extensión "Policy Constrains" de los *Certificados* raíz de las AC no es utilizada.

7.1.8. Sintaxis y semántica de los calificadores de política

336. La extensión "Certificate Policies" puede incluir hasta dos campos de "Policy Qualifiers" (detallados en cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* de las AC):

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

7.1.9. Tratamiento semántico para la extensión "certificate policy"

337. 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 la posibilidad de incorporar los dos campos relacionados en el apartado anterior en función de cada AC.

7.2. PERFIL DE LA CRL

7.2.1. Número de versión

338. 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*.

7.2.2. CRL y extensiones

339. Los perfiles de las CRL siguen la siguiente estructura:

TABLA 3 – PERFIL DE LA CRL DE LA AC RAÍZ FNMT-RCM

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	Sha256WithRSAEncryption para jerarquía AC RAIZ FNMT.
Número de CRL	Valor incremental
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión
Fecha de próxima actualización	Fecha de emisión + 24 horas (salvo la ARL que es Fecha de emisión + 6 meses)
Identificador de la clave de Autoridad	Hash de la clave del emisor
ExpiredCertsOnCRL	NotBefore de la CA
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

Tabla 4 – Perfil de la CRL de la AC RAÍZ FNMT-RCM G2

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	ecdsa-with-SHA384 para jerarquía AC RAIZ FNMT-RCM G2

Campos y extensiones	Valor
Número de CRL	Valor incremental
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión
Fecha de próxima actualización	Fecha de emisión + 24 horas (salvo la ARL que es Fecha de emisión + 6 meses)
Identificador de la clave de Autoridad	Hash de la clave del emisor
ExpiredCertsOnCRL	NotBefore de la CA
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

Tabla 5 – Perfil de la CRL de la AC RAÍZ FNMT-RCM TSA

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	ecdsa-with-SHA384 para jerarquía AC RAIZ FNMT-RCM TSA
Número de CRL	Valor incremental
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión
Fecha de próxima actualización	Fecha de emisión + 24 horas (salvo la ARL que es Fecha de emisión + 6 meses)
Identificador de la clave de Autoridad	Hash de la clave del emisor
ExpiredCertsOnCRL	NotBefore de la CA

Campos y extensiones	Valor
Punto de distribución	URLs del punto de distribución y ámbito de las CRLs
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

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

7.3.1. Número de versión

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

7.3.2. Extensiones del OCSP

342. Las respuestas OCSP del *Servicio de información y consulta sobre el estado de validez de los certificados* incluyen, para las peticiones que lo soliciten, la extensión global "nonce", que se utiliza para vincular una petición con una respuesta, de forma que se puedan prevenir ataques de repetición.

343. Adicionalmente se incluye la extensión "Extended Revoked Definition" en los casos en los que se consulta por un *Certificado* que a la AC le consta como no emitido. De esta forma, el servicio responde a la consulta de certificados no emitidos por la AC como *Certificado* revocado.

8. AUDITORÍAS DE CUMPLIMIENTO

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

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

346. El *Servicio Cualificado de Sellado de Tiempo* ofrecido por la FNMT-RCM está sujeto a auditorías anuales, según el esquema de certificación correspondiente a los *Prestadores de Servicios de Confianza*, en cuanto al cumplimiento de los requisitos definidos por los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI EN 319 421 "Trust Service Providers issuing Time-Stamps" y ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles".

347. El Servicio de firma en servidor ofrecido por la FNMT-RCM está sujeto a auditorías anuales, según el esquema de certificación correspondiente a los *Prestadores de Servicios de Confianza*, en cuanto al cumplimiento de los requisitos definidos por el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers".

348. Un auditor independiente evaluará anualmente el cumplimiento por parte de la CA de los requisitos y prácticas establecidos en esta DPC y / o los requisitos básicos y las pautas establecidas en CAB Forum's S/MIME Baseline Requirements.

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

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

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

8.1. FRECUENCIA DE LAS AUDITORÍAS

351. Las auditorías conforme a los estándares ETSI mencionadas en el apartado anterior se realizan anualmente.

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

8.2. CUALIFICACIÓN DEL AUDITOR

353. El auditor que verifique y compruebe la correcta operativa del *Prestador de Servicios de Confianza* 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. Al menos, estará acreditado según el estándar europeo ETSI EN 319 403.

354. 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.

8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA

355. 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.

356. 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.

357. 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.

8.4. ELEMENTOS OBJETOS DE AUDITORÍA

358. 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.

8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS

359. 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.

360. 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 Confianza*, la FNMT-RCM actuará según lo descrito en el Plan de continuidad de negocio, con el fin de salvaguardar la seguridad de toda la infraestructura.

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

8.6. COMUNICACIÓN DE LOS RESULTADOS

362. Las Autoridades Administrativas o Judiciales competentes podrán solicitar los informes de auditorías para verificar el buen funcionamiento del *Prestador de Servicios de Confianza*.

8.7. AUTOEVALUACIÓN

363. Adicionalmente, la FNMT-RCM realiza auditorías internas para autoevaluar el cumplimiento de sus *Políticas de Certificación*, *Declaración de Prácticas de Certificación*, normativa aplicable, y los requisitos establecidos por la entidad CA/Browser Forum, así como para controlar la calidad en la prestación de los servicios. Estas auditorías internas se llevan a cabo al menos trimestralmente, tomando una muestra seleccionada al azar, de al menos un 3% de los *Certificados* emitidos durante el periodo que comienza inmediatamente después de la muestra de autoevaluación anterior.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

364. 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 *Acuerdo* formalizado para tal efecto.

365. 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, con sujeción a su Estatuto. 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. Tarifas de emisión o renovación de certificados

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

9.1.1. Tarifas de acceso a los certificados

367. No estipulado.

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

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

9.1.3. Tarifas para otros servicios

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

9.1.4. Política de reembolso

370. Cada *Declaración de Políticas de Certificación* y *Prácticas de Certificación Particulares* podrá definir una política de reembolso para cada *Servicio de Confianza.*

9.2. RESPONSABILIDADES FINANCIERAS

371. La FNMT-RCM cuenta con los recursos humanos, materiales y financieros necesarios para cubrir los requisitos de aplicación a cada política declarada. Como Entidad Pública Empresarial adscrita al Ministerio de Hacienda y Función Pública, en materia patrimonial le es de aplicación la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas y su Estatuto (actualmente aprobado mediante el Real Decreto 51/2023, de 31 de enero), en cuanto a la adecuación, suficiencia, aplicación efectiva, identificación y control de sus bienes para servir al servicio público a que están destinados. Adicionalmente, si bien la normativa nacional en materia de prestación de *Servicios de Confianza* establece la exención de la FNMT-RCM, debido a su carácter público, de constitución de un seguro de responsabilidad civil para ejercer como *Prestador cualificado de servicios electrónicos de confianza*, esta Entidad cuenta, de manera voluntaria, con dicho seguro, según se define en el siguiente apartado.

9.2.1. Seguro de responsabilidad civil

372. FNMT-RCM, como *Prestador de Servicios de Confianza*, 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 Confianza*, con un límite de cobertura superior a 4.000.000 Euros.

9.2.2. Otros activos

373. No estipuladas.

9.2.3. Seguros y garantías para entidades finales

374. No estipuladas.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

9.3.1. Alcance de la información confidencial

375. La FNMT-RCM cuenta con normativa interna que desarrolla el "Sistema de Gestión de la Seguridad de la Información" de la Entidad, donde se define la clasificación de la información y su tratamiento.

9.3.2. Información no incluida en el alcance

376. La siguiente información es considerada no confidencial:

- La contenida en los documentos clasificados como "Público".
- La contenida en los *Certificados*.
- Las listas de revocación de *Certificados* (CRLs) y la información contenida en las respuestas del *Servicio de información y consulta sobre el estado de validez de los certificados*.
- Cualquier información cuya publicidad sea impuesta normativamente.

9.3.3. Responsabilidad para proteger la información confidencial

377. La comunicación de información confidencial relativa a la actividad del *Prestador de Servicios de Confianza* estará sujeta a la legislación vigente. La información relativa a la actividad en relación con la expedición y gestión de los *Certificados* podrá ser comunicada, en caso de requerimiento, como evidencia de certificación en caso de un procedimiento judicial, incluso sin consentimiento del *Titular* del *Certificado,* siempre que sea conforme a la legislación aplicable a esta materia.

9.4. PROTECCIÓN DE DATOS PERSONALES

378. La FNMT-RCM publica su Registro de Actividades del Tratamiento y el resto de la información relativa a datos de carácter personal, para su consulta por parte de las partes interesadas, en el siguiente sitio web: http://www.fnmt.es/politica-privacidad

9.4.1. Plan de privacidad

379. El tratamiento de datos de carácter personal que realiza la FNMT-RCM se alinea con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD), así como con los requisitos que sean de aplicación por normativa nacional específica en esta materia.

9.4.2. Información tratada como privada

380. La FNMT-RCM considera como privada toda la información personal sobre las personas físicas usuarias de los *Servicios de Confianza* que no deba ser incorporada en los certificados y en los mecanismos que utiliza el *Servicio de información y consulta sobre el estado de validez de los certificados*.

381. En todo caso, es considerada información privada toda información personal recabada en los procesos de solicitud, renovación y revocación de certificados electrónicos (con la salvedad indicada en el siguiente apartado), las *Claves Privadas* que obrasen en poder del *Prestador de Servicios de Confianza*, así como toda aquella claramente identificada como tal.

382. La FNMT-RCM aplica las salvaguardas apropiadas para proteger la información privada.

9.4.3. Información no considerada privada

383. No se considera información privada aquella que se incorpora a los certificados electrónicos, la información relativa al estado de vigencia de los mismos, la fecha de inicio de dicho estado (activo, revocado, caducado…), así como el motivo que provocó el cambio de estado. Por tanto, los *Certificados* electrónicos, las *Listas de Certificados Revocados* y cualquier contenido de los mismos no es considerada información privada.

9.4.4. Responsabilidad de proteger la información privada

384. La FNMT-RCM adopta las medidas de seguridad requeridas de conformidad con el RGPD en cuanto al acceso y tratamiento que realiza sobre los datos personales de solicitantes y suscriptores de los Certificados.

385. Las medidas técnicas y organizativas se establecerán teniendo en cuenta el coste de la técnica, los costes de aplicación, así como la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos para los derechos y libertades.

9.4.4.1. Delegado de Protección de Datos

386. El RGPD establece la obligación de designar un Delegado de Protección de Datos (DPD) a toda autoridad u organismo del sector público que lleve a cabo tratamiento de datos personales. Los datos de contacto del DPD de la FNMT-RCM están publicados en el sitio web referenciado en el primer punto del presente apartado "9.4 Protección de datos personales". Dichos datos de contacto incluyen la dirección de correo electrónico a la que los interesados pueden dirigir todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos, de conformidad con el artículo 38.4 del RGPD.

9.4.4.2. Registro de actividades de tratamiento

387. La FNMT-RCM cuenta con un registro de las actividades de tratamiento que realiza bajo su responsabilidad, entre los que se encuentra el de "gestión de la PKI" relativo a la actividad que realiza esta Entidad como *Prestador de Servicios de Confianza*. Dicho registro incluye, para cada tratamiento identificado, la siguiente información:

a. Finalidad
b. Entidad responsable
c. Categorías de datos personales
d. Quién proporciona los datos
e. Quién es el afectado de los datos personales
f. Quiénes son los encargados del tratamiento
g. Comunicaciones de datos
h. Transferencias internacionales de datos
i. Plazo de supresión
j. Medidas de seguridad

388. El documento de Registro de actividades de tratamiento puede consultarse en el sitio web referenciado en el primer punto del presente apartado "9.4 Protección de datos personales".

9.4.4.3. Derechos de los interesados

389. Los interesados podrán ejercer los derechos de acceso, rectificación, supresión, limitación de tratamiento, oposición y portabilidad de los datos, conforme a lo establecido en los artículos 15 a 22 del RGPD, dirigiéndose al responsable del tratamiento por vía electrónica, a través de la sede electrónica de la FNMT-RCM, o presencialmente a través del Registro General de dicha Entidad.

9.4.4.4. Cooperación con las Autoridades

390. La FNMT-RCM cooperará con la Agencia Española de Protección de Datos cuando sea requerida.

9.4.4.5. Notificación de violaciones de seguridad

391. La FNMT-RCM notificará a la Agencia Española de Protección de Datos (AEPD) cualquier violación de seguridad[2] en materia de datos personales, sin dilación posible y, en todo caso, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella, siempre que esta sea susceptible de constituir un riesgo para los derechos las libertades de las personas físicas afectadas.

392. En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la AEPD se complementará con una notificación dirigida a estos últimos, al objeto de permitirles la adopción de medidas para protegerse de sus consecuencias.

9.4.5. Aviso y consentimiento para usar información privada

393. La obtención de información privada de las personas físicas en los procesos ligados al ciclo de vida de los Certificados (solicitud, acreditación de la identidad, renovación, revocación…) se realizará, en cualquier caso, previa obtención del consentimiento de dichas personas de forma inequívoca, es decir, mediante una manifestación del interesado o mediante una clara acción afirmativa.

9.4.6. Divulgación conforme al proceso judicial o administrativo

394. La FNMT-RCM no divulgará datos personales, salvo petición por parte de las autoridades administrativas o judiciales.

9.4.7. Otras circunstancias de divulgación de información

395. No estipuladas.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

396. 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

[2] Según el RGPD, violación de seguridad de los datos incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

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.

397. El acceso a los servicios de *Sellado de Tiempo* estará restringido según lo dispuesto en las políticas y prácticas particulares que regulen dichos servicios.

398. 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 Servicios de Confianza y de Certificación electrónica*" - *DGPC*, 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. Queda prohibido cualquier uso distinto de la visualización, incluyendo la reproducción, redistribución y/o modificación de la presente *DGPC* así como de los documentos declarativos (políticas y prácticas) que particularizan y completan esta *DGPC,* sin la expresa autorización de la FNMT-RCM.

399. Los *OID* utilizados en los *Certificados* emitidos, en los *Certificados* empleados para la prestación de los servicios, en los *Sellos de tiempo electrónicos* 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

400. 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*.

401. 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.

402. 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*.

9.6. OBLIGACIONES Y GARANTÍAS

403. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, del *Titular* del *Certificado* y del resto de participantes, quedarán determinadas, principalmente, por el documento relativo a las condiciones de utilización o el contrato de expedición del *Certificado*, y, subsidiariamente, por la presente *DGPC* y las correspondientes *Políticas y Prácticas de Certificación* Particulares. No obstante, y con carácter general, se

describen a continuación las obligaciones de los participantes en el proceso de emisión y aceptación de los *Certificados*.

9.6.1. Obligaciones de la AC

9.6.1.1. Con carácter previo a la emisión del Certificado

404. a) Comprobar la identidad y circunstancias personales de los *Titulares* de *Certificados* con arreglo a lo dispuesto en la presente *Declaración de Prácticas y Políticas de Certificación*. No se emitirán *Certificados* para menores de edad salvo que ostenten y acrediten su cualidad de emancipados.

b) Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.

c) Comprobar que el interesado en solicitar la emisión de un *Certificado* posee el control de la *Clave Privada* que constituirá, una vez emitido el *Certificado*, los *Datos de creación de Firma* correspondientes a los de *Datos de verificación de Firma* que constarán en el *Certificado*, y comprobar su complementariedad.

d) Verificar que el *Solicitante* tiene el derecho de usar o controlar la dirección de correo electrónico contenida en la solicitud del *Certificado*.

9.6.1.2. Identificación del Titular

405. a) Identificar a la persona física que solicite un *Certificado* exigiendo, con carácter general, su personación y estar en posesión del número de Documento Nacional de Identidad, Número de Identificación de Extranjeros o, si se especifica, un documento oficial que pueda ser legalmente equivalente. Para la identificación se procederá con arreglo al procedimiento de registro aprobado por la FNMT-RCM para esta finalidad.

b) En los procesos de comprobación de los extremos antes señalados anteriormente la FNMT-RCM podrá realizar estas comprobaciones mediante la intervención de *Oficinas de Registro* autorizadas.

9.6.1.3. Generación de Datos de creación de Firma e información adicional

406. a) Garantizar que los procedimientos seguidos aseguran que las *Claves Privadas* que constituyan los *Datos de creación de Firma* son generadas manteniendo el exclusivo control por parte del *Titular*.

b) Poner a disposición del *Solicitante* (http://www.cert.fnmt.es/) la siguiente información:

i. Instrucciones para el *Titular*, en especial:

- La forma en que ha de custodiarse la información necesaria para acceder a los *Datos de creación de Firma*.
- Los mecanismos generales que garanticen la fiabilidad de la *Firma electrónica* de un documento.

- El procedimiento para comunicar la pérdida de acceso o utilización indebida de dichos Datos.
- Las condiciones precisas de utilización del *Certificado*, sus límites de uso y la forma en que garantiza su responsabilidad patrimonial.

ii. Una descripción del método utilizado por la FNMT-RCM para comprobar la identidad del *Titular* y aquellos otros datos que figuren en el *Certificado*.

iii. Las certificaciones que haya obtenido la FNMT-RCM.

iv. El procedimiento aplicable para la resolución de conflictos.

v. Un ejemplar de la presente *Declaración de Prácticas y Políticas de Certificación*, disponible a través de la *Sede Electrónica* de la FNMT-RCM.

9.6.1.4. Conservación de la información por la FNMT-RCM

407. a) Conservar toda la información y documentación relativa a cada *Certificado*, en las debidas condiciones de seguridad, durante quince (15) años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

b) Mantener un repositorio seguro y actualizado de *Certificados* en el que se identifican los *Certificados* expedidos, así como su vigencia, incluyendo en forma de *Listas de Revocación* la identificación de los *Certificados* que hayan sido revocados o suspendidos. La integridad de este *Directorio* se protegerá mediante la utilización de sistemas conformes con las disposiciones reglamentarias específicas que al respecto se dicten en España y, en su caso, en la UE.

c) Mantener un *Servicio de información y consulta sobre el estado de validez de los certificados*.

d) Establecer un mecanismo de fechado que permita determinar con exactitud la fecha y la hora en las que se expidió un *Certificado*, o se extinguió o suspendió su vigencia.

e) Conservar la presente *Declaración de Prácticas y Políticas de Certificación* durante 15 años desde su modificación o derogación por publicación de una nueva Declaración, en las debidas condiciones de seguridad.

9.6.1.5. Protección de los Datos de Carácter Personal

408. La FNMT-RCM se compromete a conocer y cumplir la legislación vigente en materia de Protección de Datos Personales y a cumplir con las obligaciones que tal normativa establece en materia de información a los afectados. Asimismo, garantiza que la utilización de los datos personales recabados se limitará a aquellas finalidades para las cuales estos fueron recogidos.

9.6.2. Obligaciones de la AR

409. Las *Oficinas de Registro*, dependientes de la *Autoridad de Registro* de la FNMT – RCM, tienen la obligación de:

i) Comprobar fehacientemente la identidad y cualesquiera circunstancias personales de los *Solicitantes* de los *Certificados* relevantes para el fin propio de estos, utilizando cualquiera de los medios admitidos en Derecho, y conforme a lo previsto en la presente DGPC.

ii) Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación o revocación gestiona durante el plazo de tiempo establecido en la legislación vigente.

iii) Permitir a la FNMT-RCM el acceso a los archivos y la auditoría de sus procedimientos en relación con los datos obtenidos en calidad de *Oficina de Registro*.

iv) Informar a la FNMT-RCM de cualquier aspecto que afecte a los *Certificados* expedidos por dicha Entidad (ej.: solicitudes de expedición, renovación…).

v) Comunicar a la FNMT-RCM de forma diligente las solicitudes de expedición de *Certificados*.

vi) Respecto de la extinción de la validez de los Certificados:

1. Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.
2. Comunicar a la FNMT-RCM de forma diligente las solicitudes de revocación de los *Certificados*.

vii) Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado correspondiente de la presente *Declaración de Prácticas y Políticas de Certificación*.

viii) Las *Oficinas de Registro*, a través del personal adscrito al servicio por relación laboral o funcionarial, deberán ejercer funciones públicas de acuerdo con la legislación específica aplicable a la FNMT-RCM. (Ley 66/1997, de 30 de diciembre, art. 81).

410. En todo caso la FNMT-RCM podrá repetir contra la *Oficina de Registro* que hubiera realizado el procedimiento de identificación, iniciando las acciones correspondientes, si la causa del daño tuviera su origen en la actuación dolosa o culposa de ésta.

9.6.3. Obligaciones de los titulares

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

412. El Solicitante mantendrá a salvo y defenderá a su costa a la FNMT-RCM contra cualquier acción que pudiese emprenderse contra esta Entidad como consecuencia de la falsedad de la información suministrada en el mencionado procedimiento de expedición del Certificado, o contra cualquier daño y perjuicio que sufra la FNMT-RCM como consecuencia de un acto u omisión del Solicitante.

413. El *Titular* del *Certificado* debe cumplir las normas de seguridad relacionadas con la custodia y uso de la información que garantiza el acceso a sus *Claves Privadas*.

414. La FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza* cuando la legislación vigente así lo permita, contemple o lo requiera, podrá recabar la dirección de correo electrónico, el número de teléfono móvil donde recibir mensajes de texto y el 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.

415. 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.

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

417. Será responsabilidad del Titular informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el *Certificado*, para su revocación y nueva expedición.

418. Asimismo, será el Titular quien deba responder ante los miembros de la Comunidad electrónica y demás Entidades usuarias o, en su caso, ante terceros del uso indebido del *Certificado*, o de la falsedad de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

419. Será responsabilidad y, por tanto, obligación del *Titular* no usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de Certificados y no se hubiera producido la subrogación prevista en la ley. En todo caso, el Titular no usará el *Certificado* en los casos en los que *los Datos de Creación de Firma / Sello* del Prestador puedan estar amenazados y/o comprometidos, y así se haya comunicado por el Prestador o, en su caso, el *Titular* hubiera tenido noticia de estas circunstancias.

9.6.4. Obligaciones de las partes que confían

420. El resto de la *Comunidad Electrónica*, *Entidades usuarias* y los terceros regularán sus relaciones con la FNMT-RCM a través de la DGPC, y, en su caso, a través de la presente *Declaración de Prácticas y Políticas de Certificación*; todo ello sin perjuicio de lo dispuesto en la normativa sobre *Firma electrónica* y demás normativa que resulte de aplicación.

421. Sin perjuicio de lo contenido en el párrafo anterior los miembros de la *Comunidad Electrónica*, *Entidades usuarias* y los terceros que confían en los *Certificados* y en las *Firmas electrónicas* generadas con los mismos, deberán cumplir las siguientes obligaciones, exonerando de cualquier responsabilidad al *Prestador de Servicios de Confianza* en caso de que alguna no sea cumplida:

- Cuando se trate de un *Certificado Cualificado*, verificar que el identificador del servicio es el que se encuentra publicado en la correspondiente *Trusted Service List*, accesibles a través del siguiente enlace:

https://esignature.ec.europa.eu/intl-comp-tl-browser/#/screen/trusted-list-provider/ES

- Verificar con carácter previo a confiar en los *Certificados*, la *Firma electrónica* o el *Sello electrónico* avanzados del *Prestador de Servicios de Confianza* que expidió el *Certificado*.
- Verificar que el *Certificado* del *Titular* continúa vigente.
- Verificar el estado de los *Certificados* en la *cadena de certificación*, mediante consulta al *Servicio de información y consulta sobre el estado de validez de los certificados* de la FNMT-RCM.
- Comprobar las limitaciones de uso contenidas en el *Certificado* que se verifica.
- Conocer las condiciones de utilización del *Certificado* conforme a la presente *Declaración de Prácticas y Políticas de Certificación*.
- Notificar a la FNMT-RCM o a cualquier *Oficina de Registro*, cualquier anomalía o información relativa al *Certificado* y que pueda ser considerada como causa de revocación del mismo, aportando todos los elementos probatorios de los que disponga.

422. Será responsabilidad de la *Entidad usuaria* y de los terceros que confíen en *Certificados* expedidos por la FNMT-RCM, salvo contratación de esta obligación con esta Entidad, la verificación de las *Firmas electrónicas* de los documentos, así como de los *Certificados*, no cabiendo en ningún caso presumir la autenticidad de los documentos o *Certificados* sin dicha verificación.

423. No podrá considerarse que la *Entidad usuaria* ha actuado con la mínima diligencia debida si confía en una *Firma electrónica* basada en un Certificado emitido por la FNMT-RCM sin haber observado lo dispuesto en la presente *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC) y* comprobado que dicha *Firma electrónica* puede ser verificada por referencia a una *Cadena de certificación* válida.

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

425. Asimismo, será responsabilidad de la *Entidad usuaria* observar lo dispuesto en la presente *DGPC* y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados*.

9.6.5. Obligaciones de otros participantes

426. La FNMT-RCM en la prestación de su servicio como *Autoridad de Sellado de Tiempo*, se responsabiliza de la variación de la referencia temporal, en relación a la proporcionada por la Sección de Hora del Real Instituto y Observatorio de la Armada, que introduce en los Sellos de tiempo electrónicos en el momento de la solicitud, más no de la veracidad ni de los contenidos representados por los datos electrónicos remitidos por las *entidades usuarias* del servicio, que son el objeto del Sello de tiempo electrónico emitido.

9.7. RENUNCIA DE GARANTÍAS

427. No estipulado.

9.8. LIMITACIONES DE RESPONSABILIDAD

428. La FNMT-RCM únicamente responde de la correcta identificación personal del *Solicitante* y futuro *Titular*, y de incorporar esos datos a un *Certificado*. Para la aplicación de garantías, obligaciones y responsabilidades, es necesario que el hecho se haya producido en el ámbito de la *Comunidad Electrónica*.

429. La FNMT-RCM únicamente responderá por deficiencias en los procedimientos propios de su actividad como *Prestador de Servicios de Confianza*, y conforme a lo dispuesto en estas *Políticas de Certificación* o en la Ley. En ningún otro caso será responsable de las acciones o de las pérdidas en las que incurran los *Titulares*, *Suscriptores*, *Entidades usuarias*, o terceros involucrados, que no se deban a errores imputables a la FNMT-RCM en los mencionados procedimientos de expedición y/o de gestión de los *Certificados*.

430. FNMT-RCM no responderá en caso de fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT-RCM podrá establecer cláusulas de limitación de responsabilidad. En todo caso, la cuantía que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial la FNMT-RCM a terceros perjudicados, y/o miembros de la *Comunidad electrónica* en defecto de regulación específica en los contratos o convenios, se limitan a un máximo de SEIS MIL EUROS (6.000€) euros.

431. La FNMT-RCM no responderá ante personas cuyo comportamiento en la utilización de los *Certificados* haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la presente *Declaración de Prácticas y Políticas de Certificación* y, en especial, lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

432. La FNMT-RCM no responderá por ningún software que no haya proporcionado directamente. No obstante, la FNMT-RCM pondrá las medidas de protección adecuadas para la protección de sus sistemas frente a *Software malicioso (Malware)* y las mantendrá diligentemente actualizadas para colaborar con los usuarios en evitar los daños que este tipo de software puede causar.

433. La FNMT-RCM no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y* en la Ley.

434. La *FNMT-RCM* en la prestación de su servicio como *Autoridad de Sellado de Tiempo*, no será responsable de los daños y perjuicios y/o funcionamiento defectuoso que los Sellos de tiempo electrónicos emitidos por ella puedan producir en los usos que puedan realizarse, ya sean estos por culpa de los interesados o por defectos de origen de los elementos.

435. La *FNMT-RCM* en la prestación de su servicio como *Autoridad de Sellado de Tiempo*, no responderá ante personas cuyo comportamiento en la utilización del Servicio cualificado de Sellado de Tiempo y/o los propios Sellos de tiempo electrónicos haya sido negligente, debiendo considerarse a estos efectos y en todo caso como negligencia la falta de observancia de lo dispuesto en la Política y Prácticas del Servicio Cualificado de Sellado de Tiempo, y en especial, en lo dispuesto en los apartados referidos a las obligaciones y a la responsabilidad de las partes.

436. La *FNMT-RCM* en la prestación de su servicio como *Autoridad de Sellado de Tiempo*, no responderá en los supuestos de caso fortuito, fuerza mayor, atentado terrorista, huelga salvaje, así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad. En todo caso, en los correspondientes contratos y/o convenios FNMT-RCM podrá establecer cláusulas de limitación de responsabilidad adicionales a las recogidas en este documento.

437. La *FNMT-RCM* en la prestación de su servicio como *Autoridad de Sellado de Tiempo*, no responderá por ningún software que no haya proporcionado directamente.

438. La *FNMT-RCM* en la prestación de su servicio como *Autoridad de Sellado de Tiempo*, no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en las Políticas y Declaraciones de Prácticas de Servicios de Confianza y de Certificación electrónica de aplicación y en la Ley.

9.9. INDEMNIZACIONES

439. La FNMT-RCM podrá incluir, en los instrumentos jurídicos que le vinculan con el *Titular*, cláusulas de indemnidad en caso de infracción de sus obligaciones o de la legislación aplicable. A estos efectos, véase también el apartado “9.6 Obligaciones y Garantías” y “9.8 Limitaciones de Responsabilidad”.

9.9.1. Indemnización de la CA

440. No estipulado.

9.9.2. Indemnización de los Suscriptores

441. No estipulado.

9.9.3. Indemnización de las partes que confían

442. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

443. La presente *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)* entrará en vigor en el momento de su publicación.

9.10.2. Terminación

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

9.10.3. Efectos de la finalización

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

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

446. La FNMT-RCM, en su actividad como *Prestador de Servicios de Confianza,* cuando la legislación vigente así lo permita, contemple o lo requiera, podrá recabar la dirección de correo electrónico, el número de teléfono móvil donde recibir mensajes de texto y/o el domicilio de los *Titulares* en el proceso de solicitud y antes de emitir un *Certificado*.

447. Esta información se recoge con la finalidad de prestar los servicios de confianza de los que son usuarios dichos *Titulares*, y/o para notificar eventos de su interés relacionados con los servicios de la FNMT-RCM, en especial, aquellos vinculados a las revocaciones de los *Certificados* o la resolución de los contratos que la FNMT-RCM haya celebrado con dichos *Titulares*. 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.

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

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. Procedimiento para las modificaciones

449. Las modificaciones del presente documento y de las *Declaraciones de Prácticas y Políticas Particulares* serán aprobadas por la Dirección del Departamento Ceres, integrada en el Comité de Gestión del PSC. La actualización quedará reflejada en la correspondiente acta, de

conformidad con el procedimiento interno aprobado mediante el documento "Procedimiento de revisión y mantenimiento de las políticas de certificación y declaración de prácticas de servicios de confianza".

9.12.2. Periodo y mecanismo de notificación

450. El Comité de Gestión del PSC revisará anualmente dichas Declaraciones y, en cualquier caso, cada vez que deba llevarse a cabo alguna modificación de las mismas.

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

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

9.12.3. Circunstancias bajo las cuales debe cambiarse un OID

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

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

454. La FNMT-RCM atenderá cualquier solicitud, queja o reclamación por parte de sus clientes o terceros que confían en sus servicios de confianza, de conformidad con los protocolos aprobados por dicha Entidad mediante los procedimientos internos "Protocolo para la gestión de acciones correctivas, preventivas y de mejora", "Protocolo para la gestión de sugerencias, quejas y reclamaciones" y "Protocolo para la gestión de incidencias". Los datos de contacto para remitir dichas sugerencias, quejas o reclamaciones son los consignados en el apartado "1.5.2 Datos de contacto" del presente documento.

9.14. NORMATIVA DE APLICACIÓN

455. La provisión de servicios de confianza de la FNMT – RCM se regirá por lo dispuesto por las Leyes del Reino de España.

456. La normativa aplicable a las presentes prácticas de servicios de confianza es la siguiente:

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados y la Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021.

457. Adicionalmente, las prácticas de los servicios de confianza provistos por la FNMT-RCM siguen los siguientes estándares:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- ETSI TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI TS 119 411-6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.
- ETSI TS 119 312 “Electronic Signatures and Infraestructures (ESI); Cryptographic Suites”.

458. Con carácter general, los miembros de la *Comunidad Electrónica* y los *Usuarios* de los servicios de confianza 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 Servicios de Confianza y de Certificación electrónica* o relacionada con ellas, directa o indirectamente, se resolverá de conformidad con lo establecido en los correspondientes contratos, condiciones generales y/o *Acuerdos*, en los términos previstos en

el Estatuto de la entidad, aprobado por RD 51/2023, de 31 de enero (BOE núm. 27, de 1 de febrero de 2023) o el que le sustituya.

459. En caso de que los contratos, condiciones generales y/o *Acuerdos*, no especificasen sistemas de resolución de conflictos, todas las partes se someten a la jurisdicción exclusiva de los tribunales del Estado español en la ciudad de Madrid.

460. Asimismo, podrán pactarse, previa aprobación de los órganos competentes de la FNMT-RCM, procedimientos de mediación o arbitraje, de acuerdo con lo establecido en la legislación aplicable.

9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE

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

9.16. ESTIPULACIONES DIVERSAS

9.16.1. Acuerdo integro

462. Los *Titulares* y terceros que confían en los Certificados asumen en su totalidad el contenido de la presente *Declaración General de Prácticas de Servicio de Confianza y de Certificación electrónica.*

9.16.2. Asignación

463. 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.

9.16.3. Severabilidad

464. No estipulado.

9.16.4. Cumplimiento

465. No estipulado.

9.16.5. Fuerza Mayor

466. No estipulado.

9.17. OTRAS ESTIPULACIONES

467. La FNMT-RCM como *Prestador de Servicios de Confianza*, 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.

468. Los servicios de confianza 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.

469. La FNMT-RCM gestiona sus servicios de certificación y emite certificados de conformidad con la última versión de los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser Forum (que pueden consultarse en la dirección https://cabforum.org/baseline-requirements-documents/) y de conformidad con la última versión de los requisitos definidos por la entidad CA/Browser Forum en su "guía para la expedición y gestión de Certificados de Validación Extendida" (que pueden consultarse en la dirección https://cabforum.org/extended-validation/) y S/MIME Baseline Requirements (SBR) que pueden consultarse en la dirección https://cabforum.org/smime-br/.

470. 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.

471. En caso de pérdida de la certificación QSCD de alguno de los *dispositivos cualificados de creación de firma / sello* de los que estuviera utilizando la FNMT-RCM, en calidad de *Prestador* Cualificado *de Servicios de Confianza*, se tomarán las medidas oportunas para reducir al mínimo el posible impacto, informando de las mismas al organismo supervisor, paralizando la expedición de certificados sobre dichos dispositivos. FNMT-RCM revocará los certificados activos en los que las *Claves privadas* se encuentren en el QSCD afectado, notificándolo al *Suscriptor*, tal y como se indica en el apartado "6.2.1 Estándares para los módulos criptográficos".

472. La estructura organizativa de la FNMT-RCM garantiza que las unidades relacionadas con la generación de Certificados y la gestión de revocación son independientes de otras unidades que deciden sobre el establecimiento, provisión y mantenimiento y suspensión de servicios de conformidad con las políticas de certificados aplicables. El documento interno de "Organización del departamento de Ceres" define la citada estructura organizativa. Adicionalmente, la naturaleza jurídica de la FNMT-RCM, como organismo público adscrito a la Administración General del Estado, avala que la Dirección y el personal con roles de confianza, están libres de cualquier presión comercial, financiera y de otro tipo que pudiera influir negativamente en la confianza en los servicios que presta.

473. La FNMT-RCM aplica a sus servicios, procesos y procedimientos los principios de igualdad de oportunidades, no discriminación y accesibilidad universal. Las medidas adoptadas cumplen razonablemente con los criterios y condiciones básicas de accesibilidad y no discriminación de conformidad con la normativa aplicable (ver apartado "9.14. Normativa de

aplicación"), con el objetivo de garantizar que los *Usuarios* de los servicios de confianza, en ningún caso, sufren discriminación alguna en el ejercicio de sus derechos y facultades por causas basadas en razones de discapacidad o edad avanzada. Adicionalmente, los sitios web de la FNMT-RCM son sometidos a análisis en materia de cumplimiento de requisitos de accesibilidad, como por ejemplo el del Observatorio de Accesibilidad del Ministerio de Hacienda y Función Pública.

474. La FNMT-RCM permite a terceros verificar y probar todos los tipos de certificados que expide. Para ello cuenta con un conjunto de certificados de prueba que pueden ser solicitados a través de la dirección de correo electrónico que figura en el apartado "1.5.2 Datos de contacto".

475. Para proporcionar una garantía razonable de que los certificados de prueba no se usan fuera del ámbito de uso de prueba, los certificados de prueba se emiten, por defecto, con unos datos identificativos ficticios regulados por el Organismo Supervisor, usando entre otros como NIF de Organismo Q0000000J.

476. En caso de emitir certificados de pruebas con datos de identidad diferentes, se informará al Organismo Supervisor. De emitirse, estos certificados siempre tendrán una validez limitada a la duración de pruebas.

ANEXO I: PERFIL DEL CERTIFICADO RAÍZ FNMT

Campo		Contenido	Ext. Critica
1. Version		2	
2. Serial Number		Número identificativo único del certificado.	
3. Signature Algorithm		Sha256withRsaEncryption	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	
	4.1. Country	C=ES	
	4.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de confianza (emisor del certificado). O=FNMT-RCM	
	4.3. Organization Unit	OU=AC RAIZ FNMT-RCM	
5. Validity		Hasta 01/01/2030	
6. Subject			
	6.1. Country	C=ES	
	6.2. Organization	Denominación (nombre "oficial" de la organización) del prestador de servicios de confianza (emisor del certificado). O=FNMT-RCM.	
	6.3. Organization Unit	OU=AC RAIZ FNMT-RCM	
7. Subject Public Key Info		Algoritmo: RSA Encryption Longitud: 4096 bits	
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.	
9. Key Usage		Uso permitido de las claves certificadas.	Sí
	9.1. Digital Signature	0	
	9.2. Content Commitment	0	
	9.3. Key Encipherment	0	
	9.4. Data Encipherment	0	

Campo			Contenido	Ext. Critica
	9.5. Key Agreement		0	
	9.6. Key Certificate Signature		1	
	9.7. CRL Signature		1	
10. Certificate Policies			Política de certificación	
	10.1. Policy Identifier		2.5.29.32.0 (anyPolicy)	
	11.2. Policy Qualifier Id			
		11.2.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	
11. Basic Constraints				Sí
	11.1. cA		Valor TRUE (CA)	
	11.2. pathLenConstraint		Ninguna	

ANEXO II: PERFIL DEL CERTIFICADO RAÍZ FNMT G2

Campo	Contenido	Obligatorio	Criticidad
1. Versión	2	Si	
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si	
3. Signature Algorithm	ecdsa-with-SHA384	Si	
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si	
4.1. Country	C=ES	Si	
4.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si	
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J		
4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn=AC RAIZ FNMT-RCM G2	Si	
5. Validity	25 años	Si	
5.1. Not before	UTCTime YYMMDDHHMMSSZ 241010091352GMT+00:00	Si	
5.2. Not after	UTCTime YYMMDDHHMMSSZ 491004091351GMT+00:00	Si	
6. Subject		Si	
6.1. Country	C=ES	Si	
6.2. Organization	O=FNMT-RCM	Si	
6.3. OrganizationalIdentifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora.	No	

Campo	Contenido	Obligatorio	Criticidad
	organizationIdentifier=VATES-Q2826004J		
6.4. Common Name	cn= AC RAIZ FNMT-RCM G2	Sí	
7. Authority Key Identifier	Identificador de la clave pública de la CA Raíz	Sí	
7.1. Key Identifier			
8. Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp384r1.	Sí	No
9. Subject Key Identifier	Identificador de la clave pública del Firmante. Es el medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	
9.1. Key Identifier			
10. Key Usage		Sí	Sí
10.1. Digital Signature	0	Sí	
10.2. Content Commitment	0	Sí	
10.3. Key Encipherment	0	Sí	
10.4. Data Encipherment	0		
10.5. Key Agreement	0	Sí	
10.6. Key Certificate Signature	1	Sí	
10.7. CRL Signature	1	Sí	
11. Basic Constrains		Sí	Sí
11.1. CA	Entidad Final (valor TRUE)	Sí	

ANEXO III: PERFIL DEL CERTIFICADO RAÍZ FNMT TSA

Campo	Contenido	Oblig.	Crit.
1. Versión	2	Si	
2. Serial Number	Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Si	
3. Signature Algorithm	ecdsa-with-SHA384	Si	
4. Issuer Distinguish Name	Autoridad de Certificación emisora del certificado	Si	
4.1. Country	C=ES	Si	
4.2. Organization	Denominación del prestador de servicios de confianza que emite el certificado. (nombre "oficial" de la organización) o=FNMT-RCM.	Si	
4.3. Organization Identifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J		
4.4. Common Name	CA del prestador de servicios de confianza bajo la cual se generar el certificado electrónico cn=AC RAIZ FNMT-RCM TSA	Si	
5. Validity	25 años	Si	
5.1. Not before	UTCTime YYMMDDHHMMSSZ	Si	
5.2. Not after	UTCTime YYMMDDHHMMSSZ	Si	
6. Subject		Si	
6.1. Country	C=ES	Si	
6.2. Organization	O=FNMT-RCM	Si	
6.3. OrganizationalIdentifier	Número único de identificación de la entidad, aplicable de acuerdo con el país. En España, NIF de la entidad suscriptora. organizationIdentifier=VATES-Q2826004J	No	

Campo	Contenido	Oblig.	Crit.
6.4. Common Name	cn= AC RAIZ FNMT-RCM TSA	Sí	
7. Authority Key Identifier	Identificador de la clave pública de la AC Raíz	Sí	
8. Subject Public Key Info	Clave pública del Firmante, codificada de acuerdo con el algoritmo criptográfico. En este caso Secp384r1.	Sí	No
9. Subject Key Identifier	Identificador de la clave pública del Firmante. Es el medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	Sí	
10. Key Usage		Sí	Sí
10.1. Digital Signature	0	Sí	
10.2. Content Commitment	0	Sí	
10.3. Key Encipherment	0	Sí	
10.4. Data Encipherment	0		
10.5. Key Agreement	0	Sí	
10.6. Key Certificate Signature	1	Sí	
10.7. CRL Signature	1	Sí	
11. Basic Constrains		Sí	Sí
11.1. CA	Entidad Final (valor TRUE)	Sí	