Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DECLARACIÓN DE POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN DE CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	24/08/2026
Revisado por:	FNMT-RCM	24/08/2026
Aprobado por:	FNMT-RCM	24/08/2026

Versión	Fecha	Descripción
1.0	5/03/2019	Declaración de Prácticas y Políticas de Certificación de certificados de autenticación de sitios web, bajo la jerarquía de la AC Raíz FNMT SERVIDORES SEGUROS
1.1	30/05/2019	Actualización métodos de validación de dominios conforme a CA/Browser Forum Baseline Requeriments.
1.2	20/01/2020	Revisión general y actualización de mejora
1.3	16/06/2020	Revisión general conforme a Mozilla Root Store Policy v.2.7, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.7.0. y EV Guidelines v.1.7.2
1.4	31/08/2020	Reducción de la validez de los certificados SSL OV a 12 meses. Mejoras en varios apartados.
1.5	01/10/2020	Incorporación del EKU “Autenticación de cliente” a los certificados de autenticación de sitios web
1.6	26/11/2020	Incorporación de la información de la DGPC común para mayor claridad. Revisión general conforme a Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.7.3. y EV Guidelines v.1.7.4
1.7	18/02/2021	Se incorpora dirección URL donde se publicó la lista de fuentes de consulta de Agencia de Registro. Revisión de cumplimiento Ley 6/2020. Se documenta el intervalo máximo entre dos revisiones de la Política de Seguridad de la Información.
1.8	28/04/2021	Revisión general y revisión conforme a la Política Mozilla v2.7.1. – Se incorpora información en relación a los métodos para comunicar un compromiso de claves.

Versión	Fecha	Descripción
1.9	30/09/2021	Revisión general conforme a Mozilla Root Store Policy v.2.7.1, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.8.0. y EV Guidelines v.1.7.8. Se incorporan detalles en relación al ballot SC48.
1.10	02/03/2022	Incorporación de información para las terceras partes que confían en certificados cualificados.
1.11	02/03/2023	Revisión general conforme a Mozilla Root Store Policy v.2.8, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.8.6. y EV Guidelines v.1.8.0. Modificación de las referencias al nuevo estatuto RD 51/2023.
1.12	07/02/2024	Revisión general
1.13	11/04/2024	Actualización de la extensión “Certificate Policies”
1.14	03/02/2025	Revision general. Modificación de los métodos usados para la validación de la autorización y control sobre el dominio. Inclusión de detalle de los registro de eventos.
1.15	26/03/2025	Revisión general conforme a Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
1.16	28/11/2025	Revisión general. Inclusión de la sección 5.7.1.1 Planes de respuesta ante incidentes y recuperación ante desastres y 5.7.1.2 Plan de revocación masiva. Reorganización del apartado 5.7. Eliminación del método de validación por correo electrónico a contacto de dominio (3.2.2.4) Actualización, ampliación y mejorar claridad en los apdos.: 2.2 / 3.1.2 / 3.2 / 3.2.2 / 3.2.2.8 / 3.2.2.9 / 4.2.1 / 4.2.2 / 4.3.1 / 4.4.1 / 4.5.1 / 4.9.1 / 4.9.7 / 4.9.9 / 4.10.1 / 4.10.2 / 5.1.8 / 5.2.1 / 5.2.4 / 5.3.6 / 5.4.1 / 5.4.8 / 6.1.1.3 / 6.3.2 / 7.2.2 / 8.1 / 8.2 / 8.7 / 9.6.1 / 9.6.3 / 9.14 / 9.16.3. Eliminación de contenido redundante en apto. 9.17.
1.17	18/12/2025	Se añaden jerarquía G2R y subordinadas G2.
1.18	12/03/2026	Nuevos periodos de tiempo en 4.2.1 y 6.3.2. Apartado 3.2.2.4 actualizado y 3.2.2.8.1 añadido. Revisión general.
1.19	24/08/2026	Revisión general de las nuevas jerarquías.

Referencia: DPC/DPCASW_0119/SGPSC/2026

Documento clasificado como: *Público*

Índice de contenidos

1. Introducción 12

1.1. Descripción general 12

1.2. Nombre del documento e identificación 13

1.3. Partes intervinientes 15
1.3.1. Autoridad de Certificación 15
1.3.2. Autoridad de Registro 22
1.3.3. Suscriptores de los certificados 22
1.3.4. Partes que confían 22
1.3.5. Otros participantes 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 23

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 24
1.5.4. Procedimiento de aprobación de la DPC 24

1.6. Definiciones y Acrónimos 25
1.6.1. Definiciones 25
1.6.2. Acrónimos 27

2. Publicación y repositorios 28

2.1. Repositorio 28

2.2. Publicación de información de certificación 28

2.3. Frecuencia de publicación 29

2.4. Control de acceso a los repositorios 29

3. Identificación y autenticación 29

3.1. Denominación 29
3.1.1. Tipos de nombres 29
3.1.2. Significado de los nombres 30
3.1.3. Seudónimos 30
3.1.4. Reglas utilizadas para interpretar varios formatos de nombres 30
3.1.5. Unicidad de los nombres 30
3.1.6. Reconocimiento y autenticación de marcas registradas 30

3.2. Validación inicial de la identidad 30
3.2.1. Métodos para probar la posesión de la clave privada 31
3.2.2. Autenticación de la identidad de la Organización 31
3.2.2.1 Identidad 31
3.2.2.2 Nombre comercial o marca registrada 32
3.2.2.3 Verificación del país 32
3.2.2.4 Validación de la autorización y control sobre el dominio 32
3.2.2.5 Autenticación para una dirección IP 33
3.2.2.6 Validación de dominio wildcard 33

3.2.2.7 Fiabilidad de las fuentes de datos ... 33
3.2.2.8 Registro CAA ... 33
3.2.2.8.1 Validación DNSSEC de Registros CAA ... 34
3.2.2.9 Corroboración de Emisión Multi-Perspectiva ... 34
3.2.3. Autenticación de la identidad de la persona física solicitante ... 35
3.2.4. Información no verificada del Suscriptor ... 35
3.2.5. Validación de la capacidad de representación ... 35
3.2.6. Criterios de interoperación ... 36

3.3. Identificación y autenticación para peticiones de renovación de claves ... 36
3.3.1. Identificación y autenticación para renovación rutinaria de claves ... 36
3.3.2. Identificación y autenticación para renovación de claves después de una revocación ... 36

3.4. Identificación y autenticación para peticiones de revocación ... 36

4. Requisitos operativos del ciclo de vida de los certificados ... 36

4.1. Solicitud de Certificados ... 36
4.1.1. Quién puede solicitar un Certificado ... 36
4.1.2. Proceso de registro y responsabilidades ... 36

4.2. Procedimiento de solicitud de certificados ... 37
4.2.1. Realización de las funciones de identificación y autenticación ... 37
4.2.2. Aprobación o rechazo de la solicitud del certificado ... 38
4.2.3. Tiempo en procesar la solicitud ... 39

4.3. Emisión del certificado ... 39
4.3.1. Acciones de la AC durante la emisión ... 39
4.3.2. Notificación de emisión de certificado ... 39

4.4. Aceptación del certificado ... 40
4.4.1. Proceso de aceptación ... 40
4.4.2. Publicación del certificado por la AC ... 40
4.4.3. Notificación de la emisión a otras entidades ... 40

4.5. Par de claves y uso del certificado ... 40
4.5.1. Clave privada del suscriptor y uso del certificado ... 40
4.5.2. Uso del certificado y la clave pública por terceros que confían ... 40

4.6. Renovación del certificado ... 41
4.6.1. Circunstancias para la renovación del certificado ... 41
4.6.2. Quién puede solicitar la renovación del certificado ... 41
4.6.3. Procesamiento de solicitudes de renovación del certificado ... 41
4.6.4. Notificación de la renovación del certificado ... 41
4.6.5. Conducta que constituye la aceptación de la renovación del certificado ... 41
4.6.6. Publicación del certificado renovado ... 41
4.6.7. Notificación de la renovación del certificado a otras entidades ... 42

4.7. Renovación con regeneración de las claves del certificado ... 42
4.7.1. Circunstancias para la renovación con regeneración de claves ... 42
4.7.2. Quién puede solicitar la renovación con regeneración de claves ... 42
4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves ... 42
4.7.4. Notificación de la renovación con regeneración de claves ... 42
4.7.5. Conducta que constituye la aceptación de la renovación con regeneración de claves ... 42
4.7.6. Publicación del certificado renovado ... 42
4.7.7. Notificación de la renovación con regeneración de claves a otras entidades ... 42

4.8. Modificación del certificado 42
4.8.1. Circunstancias para la modificación del certificado 43
4.8.2. Quién puede solicitar la modificación del certificado 43
4.8.3. Procesamiento de solicitudes de modificación del certificado 43
4.8.4. Notificación de la modificación del certificado 43
4.8.5. Conducta que constituye la aceptación de la modificación del certificado 43
4.8.6. Publicación del certificado modificado 43
4.8.7. Notificación de la modificación del certificado a otras entidades 43

4.9. Revocación y suspensión del certificado 43
4.9.1. Circunstancias para la revocación 44
4.9.1.1 Causas de revocación de un Certificado de entidad final 44
4.9.1.2 Causas de revocación de un Certificado de CA subordinada 47
4.9.2. Quién puede solicitar la revocación 47
4.9.3. Procedimiento de solicitud de la revocación 48
4.9.4. Periodo de gracia de la solicitud de revocación 49
4.9.5. Plazo de tiempo para procesar la solicitud de revocación 50
4.9.6. Obligación de verificar las revocaciones por las partes que confían 50
4.9.7. Frecuencia de generación de CRLs 50
4.9.8. Periodo máximo de latencia de las CRLs 51
4.9.9. Disponibilidad del sistema de verificación online del estado de los certificados 51
4.9.10. Requisitos de comprobación en línea de la revocación 52
4.9.11. Otras formas de aviso de revocación disponibles 52
4.9.12. Requisitos especiales de revocación de claves comprometidas 52
4.9.13. Circunstancias para la suspensión 52
4.9.14. Quién puede solicitar la suspensión 53
4.9.15. Procedimiento para la petición de la suspensión 53
4.9.16. Límites sobre el periodo de suspensión 53

4.10. Servicios de información del estado de los certificados 53
4.10.1. Características operativas 54
4.10.2. Disponibilidad del servicio 54
4.10.3. Características opcionales 55

4.11. Finalización de la suscripción 55

4.12. Custodia y recuperación de claves 55
4.12.1. Prácticas y políticas de custodia y recuperación de claves 55
4.12.2. Prácticas y políticas de protección y recuperación de la clave de sesión 55

5. Controles de seguridad física, de procedimientos y de personal 55

5.1. Controles de Seguridad Física 56
5.1.1. Ubicación de las instalaciones 56
5.1.1.1 Situación del Centro de Proceso de Datos 56
5.1.2. Acceso Físico 56
5.1.2.1 Perímetro de seguridad física 56
5.1.2.2 Controles físicos de entrada 57
5.1.2.3 El trabajo en áreas seguras 57
5.1.2.4 Visitas 57
5.1.2.5 Áreas aisladas de carga y descarga 57
5.1.3. Electricidad y Aire Acondicionado 57
5.1.3.1 Seguridad del cableado 58
5.1.4. Exposición al agua 58
5.1.5. Prevención y Protección contra incendios 58

5.1.6. Almacenamiento de Soportes 58
5.1.6.1 Recuperación de la información 58
5.1.7. Eliminación de Residuos 58
5.1.8. Copias de Seguridad fuera de las instalaciones 59

5.2. Controles de Procedimiento 59
5.2.1. Roles de Confianza 60
5.2.2. Número de personas por tarea 60
5.2.3. Identificación y autenticación para cada rol 60
5.2.4. Roles que requieren segregación de funciones 61

5.3. Controles de Personal 61
5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos 62
5.3.2. Procedimientos de verificación de antecedentes 63
5.3.3. Requisitos de formación 63
5.3.4. Requisitos y frecuencia de actuación formativa 64
5.3.5. Secuencia y frecuencia de rotación laboral 64
5.3.6. Sanciones por acciones no autorizadas 64
5.3.7. Requisitos de contratación de personal 64
5.3.7.1 Requisitos de contratación de terceros 65
5.3.8. Suministro de documentación al personal 65

5.4. Procedimientos de auditoría 65
5.4.1. Tipos de eventos registrados 66
5.4.1.1 Registro o Log de actividades con Firewall y enrutadores 67
5.4.2. Frecuencia de procesamiento de registros 67
5.4.3. Periodo de conservación de los registros 68
5.4.4. Protección de los registros 68
5.4.5. Procedimientos de copias de seguridad de los registros auditados 68
5.4.6. Sistemas de recolección de registros 68
5.4.7. Notificación al sujeto causante de los eventos 68
5.4.8. Evaluación de vulnerabilidades 69

5.5. Archivado de registros 69
5.5.1. Tipos de registros archivados 69
5.5.2. Periodo de retención del archivo 70
5.5.3. Protección del archivo 70
5.5.4. Procedimientos de copia de respaldo del archivo 70
5.5.5. Requisitos para el sellado de tiempo de los registros 70
5.5.6. Sistema de archivo 71
5.5.7. Procedimientos para obtener y verificar la información archivada 71

5.6. Cambio de claves de la AC 71

5.7. Recuperación de desastres y compromisos 71
5.7.1. Procedimientos de manejo de incidentes y compromisos 71
5.7.1.1. Planes de respuesta ante incidentes y recuperación ante desastres 72
5.7.1.2. Plan de revocación masiva 72
5.7.2. Actuación ante recursos, software y/o datos corruptos 73
5.7.3. Procedimiento ante compromiso de la clave privada de la AC 73
5.7.4. Continuidad de negocio después de un desastre 73

5.8. Cese de la actividad del Prestador de Servicios de Confianza 74

6. Controles de seguridad técnica 75

6.1. Generación e instalación de las Claves ... *75*
6.1.1. Generación del par de claves ... 75
6.1.1.1 Generación del par de Claves de la CA ... 75
6.1.1.2 Generación del par de Claves de la RA ... 76
6.1.1.3 Generación del par de Claves de los Suscriptores ... 76
6.1.2. Envío de la clave privada al suscriptor ... 76
6.1.3. Envío de la clave pública al emisor del certificado ... 76
6.1.4. Distribución de la clave pública de la AC a las partes que confían ... 76
6.1.5. Tamaños de claves y algoritmos utilizados ... 76
6.1.6. Parámetros de generación de la clave pública y verificación de la calidad ... 77
6.1.7. Usos admitidos de las claves (KeyUsage field X.509v3) ... 77

6.2. Protección de la clave privada y controles de los módulos criptográficos ... *77*
6.2.1. Estándares para los módulos criptográficos ... 77
6.2.2. Control multi-persona (n de m) de la clave privada ... 78
6.2.3. Custodia de la clave privada ... 78
6.2.4. Copia de seguridad de la clave privada ... 78
6.2.5. Archivado de la clave privada ... 78
6.2.6. Transferencia de la clave privada a/o desde el módulo criptográfico ... 78
6.2.7. Almacenamiento de la clave privada en el módulo criptográfico ... 78
6.2.8. Método de activación de la clave privada ... 79
6.2.9. Método de desactivación de la clave privada ... 79
6.2.10. Método de destrucción de la clave privada ... 79
6.2.11. Clasificación de los módulos criptográficos ... 79

6.3. Otros aspectos de la gestión del par de claves ... *79*
6.3.1. Archivo de la clave pública ... 79
6.3.2. Periodos operativos del certificado y periodos de uso del par de claves ... 79

6.4. Datos de activación ... *80*
6.4.1. Generación e instalación de datos de activación ... 80
6.4.2. Protección de datos de activación ... 80
6.4.3. Otros aspectos de los datos de activación ... 80

6.5. Controles de seguridad informática ... *80*
6.5.1. Requisitos técnicos específicos de seguridad informática ... 80
6.5.1.1 Comunicación de las incidencias de seguridad ... 81
6.5.1.2 Comunicación de las debilidades de seguridad ... 81
6.5.1.3 Comunicación de los fallos del software ... 81
6.5.1.4 Aprendiendo de las incidencias ... 81
6.5.2. Evaluación del nivel de seguridad informática ... 81

6.6. Controles técnicos del ciclo de vida ... *82*
6.6.1. Controles de desarrollo de sistemas ... 82
6.6.2. Controles de gestión de la seguridad ... 82
6.6.3. Controles de seguridad del ciclo de vida ... 82
6.6.3.1 Actualización de algoritmia ... 82

6.7. Controles de seguridad de red ... *82*

6.8. Fuente de tiempo ... *83*

7. Perfiles de los certificados, CRLs y OCSP ... 84

7.1. Perfil del certificado ... *84*
7.1.1. Número de versión ... 84

7.1.2. Extensiones del certificado 84
7.1.3. Identificadores de objeto de algoritmos 84
7.1.4. Formatos de nombres 85
7.1.5. Restricciones de nombres 85
7.1.6. Identificador de objeto de política de certificado 85
7.1.7. Empleo de la extensión restricciones de política 86
7.1.8. Sintaxis y semántica de los calificadores de política 86
7.1.9. Tratamiento semántico para la extensión "Certificate policy" 86

7.2. Perfil de la CRL 86
7.2.1. Número de versión 86
7.2.2. CRL y extensiones 86

7.3. Perfil de OCSP 87
7.3.1. Número de versión 87
7.3.2. Extensiones del OCSP 87

8. Auditorías de cumplimiento 87

8.1. Frecuencia de las auditorías 88

8.2. Cualificación del auditor 89

8.3. Relación del auditor con la empresa auditada 89

8.4. Elementos objetos de auditoría 89

8.5. Toma de decisiones frente a detección de deficiencias 89

8.6. Comunicación de los resultados 90

8.7. Autoevaluación 90

9. Otros asuntos legales y de actividad 90

9.1. Tarifas 90
9.1.1. Tarifas de emisión o renovación de certificados 90
9.1.2. Tarifas de acceso a los certificados 91
9.1.3. Tarifas de acceso a la información de estado o revocación 91
9.1.4. Tarifas para otros servicios 91
9.1.5. Política de reembolso 91

9.2. Responsabilidad financiera 91
9.2.1. Seguro de responsabilidad civil 91
9.2.2. Otros activos 91
9.2.3. Seguros y garantías para entidades finales 92

9.3. Confidencialidad de la información 92
9.3.1. Alcance de la información confidencial 92
9.3.2. Información no incluida en el alcance 92
9.3.3. Responsabilidad para proteger la información confidencial 92

9.4. Protección de datos de carácter personal 92
9.4.1. Plan de privacidad 92
9.4.2. Información tratada como privada 93
9.4.3. Información no considerada privada 93
9.4.4. Responsabilidad de proteger la información privada 93
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 94
9.4.4.4 Cooperación con las Autoridades 94
9.4.4.5 Notificación de violaciones de seguridad 94
9.4.5. Aviso y consentimiento para usar información privada 95
9.4.6. Divulgación conforme al proceso judicial o administrativo 95
9.4.7. Otras circunstancias de divulgación de información 95

9.5. Derechos de propiedad intelectual 95

9.6. Obligaciones y garantías 96
9.6.1. Obligaciones de la AC 96
9.6.2. Obligaciones de la AR 98
9.6.3. Obligaciones de los Suscriptores 98
9.6.4. Obligaciones de las partes que confían 101
9.6.5. Obligaciones de otros participantes 102

9.7. Renuncia de garantías 102

9.8. Límites de responsabilidad 102

9.9. Indemnizaciones 103
9.9.1. Indemnización de la CA 103
9.9.2. Indemnización de los Suscriptores 103
9.9.3. Indemnización de las partes que confían 103

9.10. Periodo de validez de este documento 104
9.10.1. Plazo 104
9.10.2. Terminación 104
9.10.3. Efectos de la finalización 104

9.11. Notificaciones individuales y comunicación con los participantes 104

9.12. Modificaciones de este documento 104
9.12.1. Procedimiento para las modificaciones 104
9.12.2. Periodo y mecanismo de notificación 105
9.12.3. Circunstancias bajo las cuales debe cambiarse un OID 105

9.13. Reclamaciones y resolución de disputas 105

9.14. Normativa de aplicación 105

9.15. Cumplimiento de la normativa aplicable 106

9.16. Estipulaciones diversas 107
9.16.1. Acuerdo íntegro 107
9.16.2. Asignación 107
9.16.3. Severabilidad 107
9.16.4. Cumplimiento 107
9.16.5. Fuerza Mayor 107

9.17. Otras estipulaciones 108

Anexo I: Perfil del certificado AC RAIZ FNMT-RCM SERVIDORES SEGUROS 110

Anexo II: Perfil del certificado AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R 111

Índice de tablas

Tabla 1 – Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS 15
Tabla 2 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 1 (Certificados EV) 16
Tabla 3 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 2 (Certificados OV)..... 17
Tabla 4 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 1 G2 (Certificados EV) 18
Tabla 5 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 2 G2 (Certificados OV) 18
Tabla 6 – Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R..... 19
Tabla 7 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 2 G2R (Certificados OV) 20
Tabla 8 – Perfiles de las CRLs 86

1. INTRODUCCIÓN

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

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

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

1.1. DESCRIPCIÓN GENERAL

4. La FNMT-RCM, a través del Departamento CERES (CERtificación ESpañola), acredita ser un *Prestador Cualificado de Servicios de Confianza*, de conformidad con el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital, a través de una entidad independiente y en el marco de un esquema de certificación, de conformidad con el estándar europeo ETSI EN 319 401 "General Policy Requirements for Trust Service Providers.

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

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

6. El presente documento (PC/DPC) tiene como objeto el cumplimiento de las últimas versiones de:

   - El documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" del CA/Browser Forum (https://cabforum.org/working-groups/server/baseline-requirements/documents/)
   - El documento "Guidelines for the Issuance and Management of Extended Validation Certificates" del CA/Browser Forum (https://cabforum.org/working-groups/server/extended-validation/guidelines/),

- Las siguientes políticas:
    1. CCADB.
    2. Chrome Root Program.
    3. Mozilla Root Store.
    4. Microsoft Trusted Root Program.
    5. Apple Root Certificate Program.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

7. El presente documento se denomina "***Declaración de Políticas y Prácticas de Certificación de certificados de autenticación de sitios web***", y en adelante será citado en este documento y con el ámbito descrito en el mismo como "*Declaración de Políticas y Prácticas de Certificación*" o por su acrónimo "*PC/DPC*" como un documento que combina unas *Políticas de Certificación (PC)* y una "*Declaración de Prácticas de Certificación"(DPC).*

   Versión: 1.19

   Fecha de expedición: 24/08/2026

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

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

9. En el ámbito de la presente *PC/DPC*, la FNMT-RCM expide los siguientes tipos de *Certificados de autenticación de sitios web*, cuya descripción se encuentra en el apartado "1.6.1 Definiciones" del presente documento:

    - *Certificados de autenticación de sitios web*, con la consideración de cualificados[1] bajo políticas de validación Extendida (EV):

[1] Expedidos conforme a los requisitos establecidos en el anexo IV del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior , modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital .

Tipo de *Certificado*	Referencia / OID[2] de política
Certificado de Sede electrónica EV	1.3.6.1.4.1.5734.3.16.1.1
Certificado EV	1.3.6.1.4.1.5734.3.16.1.2
Certificado SAN EV	1.3.6.1.4.1.5734.3.16.1.3
Certificado de Sede electrónica EV G2	1.3.6.1.4.1.5734.3.16.3.1
Certificado EV G2	1.3.6.1.4.1.5734.3.16.3.2
Certificado SAN EV G2	1.3.6.1.4.1.5734.3.16.3.3

Estos certificados con la consideración de cualificados siguen las siguientes políticas asociadas:

Extended Validation Certificate Policy (EVCP) OID: 0.4.0.2042.1.4

Extended Validation (EV) guidelines certificate policy OID: 2.23.140.1.1

QEVCP-w: certificate policy for European Union (EU) qualified website authentication certificates OID: 0.4.0.194112.1.4

- *Certificados de autenticación de sitios web*, bajo políticas de validación de Organización (OV):

Tipo de *Certificado*	Referencia / OID de política
Certificado OV	1.3.6.1.4.1.5734.3.16.2.1
Certificado Wildcard OV	1.3.6.1.4.1.5734.3.16.2.2
Certificado SAN OV	1.3.6.1.4.1.5734.3.16.2.3
Certificado OV G2	1.3.6.1.4.1.5734.3.16.4.1
Certificado Wildcard OV G2	1.3.6.1.4.1.5734.3.16.4.2
Certificado SAN OV G2	1.3.6.1.4.1.5734.3.16.4.3

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

Tipo de *Certificado*	Referencia / OID de política
Certificado OV G2 RSA	1.3.6.1.4.1.5734.3.16.6.1
Certificado Wildcard OV G2 RSA	1.3.6.1.4.1.5734.3.16.6.2
Certificado SAN OV G2 RSA	1.3.6.1.4.1.5734.3.16.6.3

Estos certificados siguen las siguientes políticas asociadas:

Organizational Validation Certificate Policy (OVCP) OID: 0.4.0.2042.1.7

Organization identity Validation OID: 2.23.140.1.2.2

El *certificado OV G2* y el *certificado OV G2 RSA* tienen además la siguiente política asociada: QNCP-w: certificate policy for European Union (EU) qualified website authentication certificates OID: 0.4.0.194112.1.5

1.3. PARTES INTERVINIENTES

10. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *PC/DPC* son las siguientes:

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

1.3.1. Autoridad de Certificación

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

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

Tabla 1 – Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS

Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
Sujeto	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, ORG_ID = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES

Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
Emisor	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, ORG_ID = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Número de serie (hex)	62:F6:32:6C:E5:C4:E3:68:5C:1B:62:DD:9C:2E:9D:95
Validez	No antes: 20 de diciembre de 2018 No después: 20 de diciembre de 2043
Longitud clave pública	ECC P-384 bits
Algoritmo de firma	Sha384ECDSA
Identificador de clave	01 B9 2F EF BF 11 86 60 F2 4F D0 41 6E AB 73 1F E7 D2 6E 49

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

Tabla 2 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 1 (Certificados EV)

Certificado de la AC subordinada SERVIDORES SEGUROS TIPO 1 (Certificados EV)	
Sujeto	CN = AC SERVIDORES SEGUROS TIPO1, ORG_ID = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Emisor	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, 2.5.4.97 = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Número de serie (hex)	50:89:86:CD:B4:17:0E:FE:5C:1B:6B:D5:C8:24:EB:5B
Validez	No antes: 20 de diciembre de 2018 No después: 20 de diciembre de 2033

Certificado de la AC subordinada SERVIDORES SEGUROS TIPO 1 (Certificados EV)	
Longitud clave pública	ECC P-384 bits
Algoritmo de firma	Sha384ECDSA
Identificador de clave	8C 42 32 40 F9 79 3F 6B 13 C1 75 C6 5D EE 86 22 44 39 6F 77

Tabla 3 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 2 (Certificados OV)

Certificado de la AC subordinada SERVIDORES SEGUROS TIPO 2 (Certificados OV)	
Sujeto	CN = AC SERVIDORES SEGUROS TIPO2, ORG_ID = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Emisor	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, ORG_ID = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES
Número de serie (hex)	13:8E:6B:BE:DF:20:F5:94:5C:1B:6C:F6:29:B4:2F:4A
Validez	No antes: 20 de diciembre de 2018 No después: 20 de diciembre de 2033
Longitud clave pública	ECC P-384 bits
Algoritmo de firma	Sha384ECDSA
Identificador de clave	C5 F2 05 4E F4 37 72 E4 EA 4F 02 57 03 FD 86 96 05 AE 50 8F

Tabla 4 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 1 G2 (Certificados EV)

Certificado de la AC subordinada SERVIDORES SEGUROS TIPO 1 G2 (Certificados EV)	
Sujeto	CN=AC SERVIDORES SEGUROS TIPO1 G2 ,ORG_ID=VATES-Q2826004J,O=FNMT-RCM,C=ES
Emisor	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS,ORG_ID=VATES-Q2826004J,OU=Ceres,O=FNMT-RCM,C=ES
Número de serie (hex)	13:0B:09:E0:F3:C7:40:39:77:07:B9:6F:9C:FB:3F:38:E8:57:31:79
Validez	No antes: 16 de diciembre de 2025 No después: 14 de diciembre de 2035
Longitud clave pública	ECC P-384 bits
Algoritmo de firma	Sha384ECDSA
Identificador de clave	73 9A 95 1C 31 89 30 5B 8C 37 18 AC 72 BD 40 76 92 C5 DF B7

Tabla 5 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 2 G2 (Certificados OV)

Certificado de la AC subordinada SERVIDORES SEGUROS TIPO 2 G2 (Certificados OV)	
Sujeto	CN=AC SERVIDORES SEGUROS TIPO2 G2,ORG_ID =VATES-Q2826004J,O=FNMT-RCM,C=ES
Emisor	CN = AC RAIZ FNMT-RCM SERVIDORES SEGUROS, ORG_ID = VATES-Q2826004J, OU = Ceres, O = FNMT-RCM, C = ES

Certificado de la AC subordinada SERVIDORES SEGUROS TIPO 2 G2 (Certificados OV)	
Número de serie (hex)	68:7B:08:83:1A:DD:AC:39:CC:28:23:F0:40:1B:32:E7:FD:A0:11:56
Validez	No antes: 16 de diciembre de 2025 No después: 14 de diciembre de 2035
Longitud clave pública	ECC P-384 bits
Algoritmo de firma	Sha384ECDSA
Identificador de clave	42 4A 37 E8 44 AC EC 39 6D 35 98 E1 AA 16 2F D8 08 A7 DA 31

c) Autoridad de Certificación raíz G2R. Dicha Autoridad expide exclusivamente *Certificados* de Autoridades de Certificación subordinadas. El certificado raíz de esta AC viene identificado por la siguiente información:

Tabla 6 – Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R

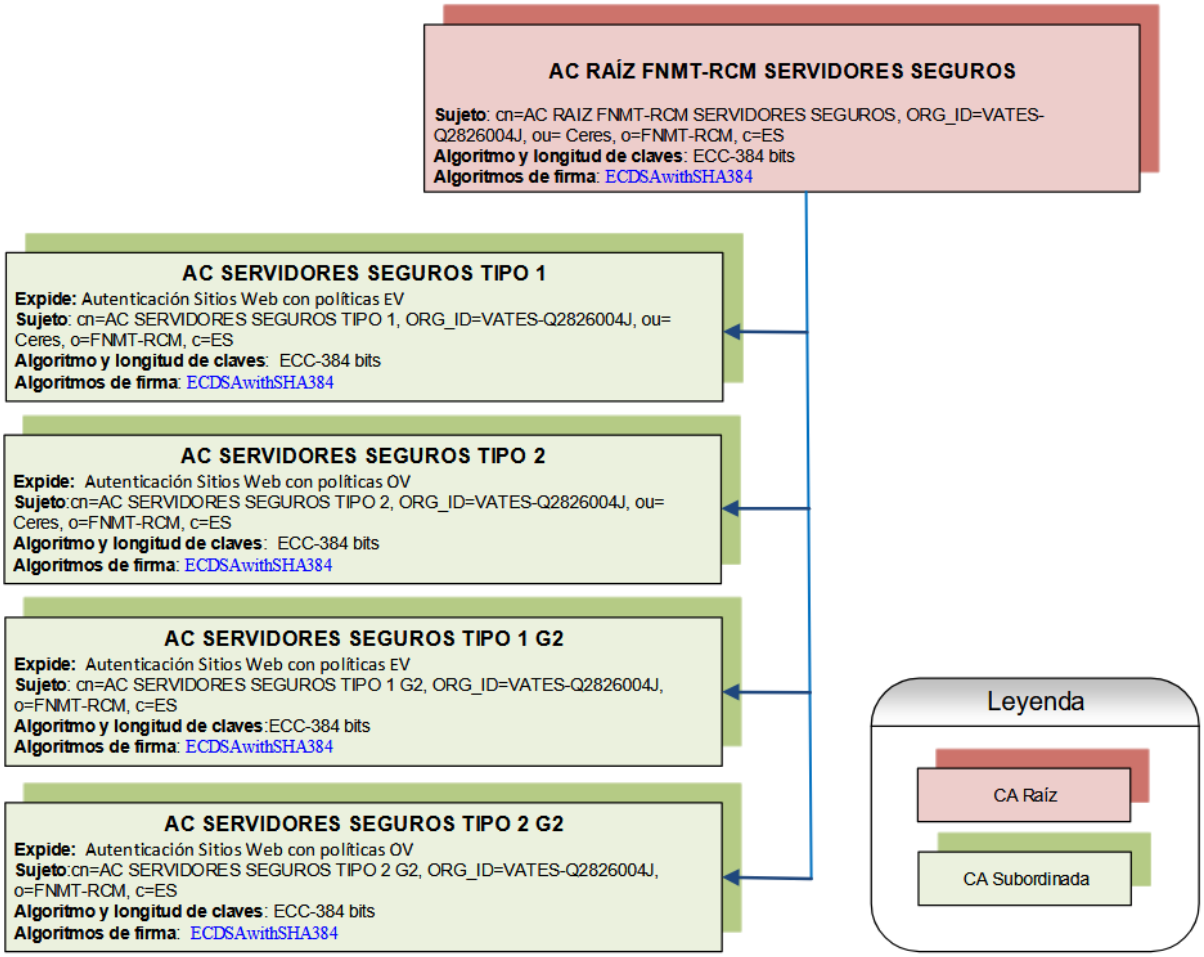
Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R	
Sujeto	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R,O=FNMT-RCM,C=ES
Emisor	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R,O=FNMT-RCM,C=ES
Número de serie (hex)	2A:0E:1C:A4:D4:B6:84:F8:A8:5A:03:C0:7F:48:41:74:E6:69:CF:40
Validez	No antes: 16 de diciembre de 2025 No después: 12 de diciembre de 2040

Certificado de la AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R	
Longitud clave pública	RSA 4096 bits
Algoritmo de firma	Sha384 with RSA
Identificador de clave	23 82 54 54 30 61 4C A0 4E 81 B9 83 88 F2 CA 05 F6 19 B8 9B

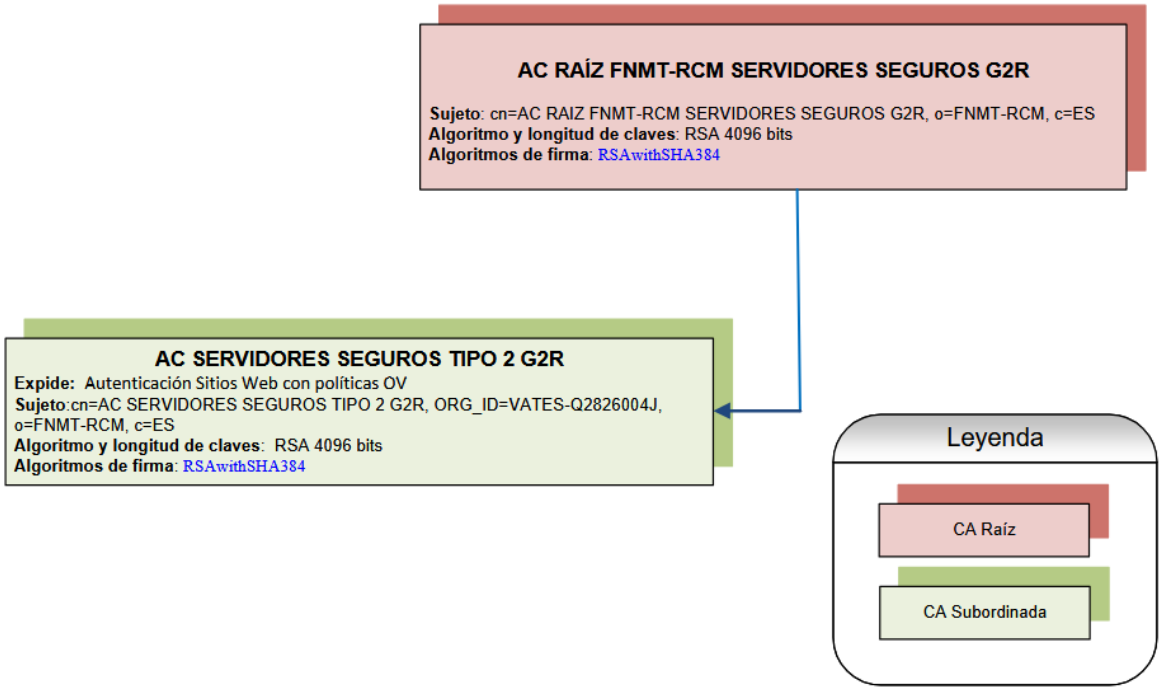
d) Autoridades de Certificación subordinadas G2R: expiden los *Certificados* de entidad final G2R objeto de la presente *PC/DPC*. Los certificados de dichas Autoridades vienen identificados por la siguiente información:

Tabla 7 – Certificado de AC subordinada SERVIDORES SEGUROS TIPO 2 G2R (Certificados OV)

Certificado de la AC subordinada SERVIDORES SEGUROS G2R (Certificados OV)	
Sujeto	CN=AC SERVIDORES SEGUROS TIPO2 G2R,ORG_ID =VATES-Q2826004J,O=FNMT-RCM,C=ES
Emisor	CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R,O=FNMT-RCM,C=ES
Número de serie (hex)	7C:B7:F3:E7:FC:87:5B:54:76:5C:06:21:FB:55:FB:8D:2E:84:C7:D1
Validez	No antes: 16 de diciembre de 2025 No después: 14 de diciembre de 2035
Longitud clave pública	RSA 4096 bits
Algoritmo de firma	Sha384 with RSA
Identificador de clave	1E 47 88 D6 39 AB 38 CD D6 C1 B1 7B 4C 35 91 DA 10 0E 16 A9



Jerarquía AC RAÍZ FNMT-RCM SERVIDORES SEGUROS



Jerarquía AC RAÍZ FNMT-RCM SERVIDORES SEGUROS G2R

1.3.2. Autoridad de Registro

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

1.3.3. Suscriptores de los certificados

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

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

1.3.4. Partes que confían

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

1.3.5. Otros participantes

16. No estipulado.

1.4. USO DE LOS CERTIFICADOS

1.4.1. Usos permitidos de los certificados

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

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

19. Todos los *Certificados de autenticación de sitios web* con políticas de Validación Extendida (EV) expedidos bajo la presente *Política de Certificación* son *Certificados Cualificados* conforme al Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital y de conformidad con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-4 "Certificate profile for web site certificates".

1.4.2. Restricciones en el uso de los certificados

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

21. La FNMT-RCM prohíbe el uso de los *Certificados* emitidos bajo la presente *PC/DPC* para la intercepción ilegal o descifrado de comunicaciones cifradas (MITM), inspección profunda de paquetes (DPI), etc.

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

- Firmar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
- Firmar software o componentes.
- Generar *Sellos de tiempo* para procedimientos de *Fechado electrónico.*

- Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como serían a título enunciativo y no limitativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación.*
    - Prestar servicios de notificación

1.5. ADMINISTRACIÓN DE POLÍTICAS

1.5.1. Entidad responsable

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

1.5.2. Datos de contacto

24. 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

25. 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

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

1.5.4. Procedimiento de aprobación de la DPC

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

28. La FNMT-RCM revisará sus políticas y prácticas de certificación y actualizará anualmente la presente Declaración de la Política de Certificados para mantenerla acorde a la última versión

de los referidos requisitos, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.

29. Las actualizaciones tanto para las Prácticas de Certificación Particulares, como para la Política de Certificación se ponen a disposición de las partes, publicando nuevas versiones en https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

1.6. DEFINICIONES Y ACRÓNIMOS

1.6.1. Definiciones

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

- *Certificado de autenticación de sitios web:* Es un *Certificado* que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el *Certificado.*
- *Certificado de autenticación de sitios web G2:* Son los *Certificados de autenticación de sitios web* generados por las "AC Servidores Seguros Tipo1 G2" o "AC Servidores Seguros Tipo2 G2" (*Certificado de Sede electrónica EV G2, Certificado EV G2, Certificado SAN EV G2, Certificado OV G2, Certificado Wildcard OV G2, Certificado SAN OV G2*).
- *Certificado de autenticación de sitios web G2 RSA:* Son los *Certificados de autenticación de sitios web* con claves RSA, generados por la "AC Servidores Seguros Tipo2 G2R" (*Certificado OV G2, Certificado Wildcard OV G2, Certificado SAN OV G2)*
- *Certificado de sede electrónica*: *Certificado EV* que identifica a una *Sede electrónica,* garantizando la comunicación segura con la misma en los términos definidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- *Certificado EV: Certificado de autenticación de sitios web* que contiene información validada del *Titular* del mismo conforme al procedimiento de validación exhaustiva de acuerdo con los requisitos de la "Guía para la emisión y gestión de Certificados de Validación Extendida" establecidos por la entidad CA/Browser forum y que pueden consultarse en la siguiente dirección https://cabforum.org/extended-validation/
- *Certificado OV: Certificado de autenticación de sitios web* expedido según la política de validación de Organización (OVCP), garantizando razonablemente al usuario de navegadores de Internet que el titular del sitio web al que accede coincide con la Organización identificada por el *Certificado OV*. Este *Certificado* cumple con los requisitos del estándar europeo ETSI EN 319 411-1 "Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- *Certificado SAN EV: Certificado EV* que incorpora un conjunto de dominios independientes entre sí.
- *Certificado SAN OV: Certificado OV* que incorpora un conjunto de dominios independientes entre sí.
- *Certificado Wildcard OV: Certificado OV* que incorpora un conjunto de subdominios ilimitado, a partir del tercer nivel, con un único *Certificado de autenticación de sitio web*.

- *Certificate Transparency (CT)*: es un marco abierto para la supervisión de *Certificados de autenticación de sitio web,* de forma que cuando se expide uno de estos *Certificados*, se publica en registros CT, posibilitando así que los propietarios de dominios puedan supervisar la emisión de los mismos para sus dominios y detectar *Certificados* emitidos erróneamente.
- *Corroboración de Emisión Multi-Perspectiva:* Proceso por el que las confirmaciones hechas durante la validación de dominio y las comprobaciones de *Registro CAA* por la *Perspectiva de Red* Primaria se corroboran por otras *Perspectivas de Red* antes de emitir el *Certificado.*
- *Declaración de Prácticas de Certificación (DPC):* Declaración puesta a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita por parte de la FNMT-RCM. Tiene la consideración de documento de seguridad en el que se detallan, en los marcos eIDAS y eIDAS2, las obligaciones que los *Prestadores de Servicios de Confianza* se comprometen a cumplir en relación con la gestión de los *Datos de creación y verificación de firma* y de los *Certificados electrónicos*, las condiciones aplicables a la solicitud, expedición, uso y extinción de la vigencia de los *Certificados*, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los *Certificados.*
- *Informe de incidencia sobre certificado (CPR):* 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
- *Non-Reserved LDH Label*: De RFC 5890: “Conjunto de etiquetas LDH válidas que no tienen "-" en la tercera y cuarta posición.”
- *Perspectiva de Red*: Relacionado con la *Corroboración de Emisión Multi-Perspectiva.* Un sistema (por ejemplo, una instancia de servidor en la nube) o colección de componentes de red (por ejemplo, una VPN y su infraestructura correspondiente) para el envío de tráfico de Internet de salida con un método de validación de dominio y/o un chequeo CAA. La ubicación de la *Perspectiva de Red* se determina por el punto en el que el tráfico no encapsulado de Internet de salida normalmente se trasfiere a la infraestructura de red que provee de conectividad a Internet a esa perspectiva.
- *Organismo de supervisión:* organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el artículo 17 del Reglamento eIDAS. En España, actualmente es el Ministerio para la Transformación Digital y de la Función Pública.
- *P-Label*: Etiqueta “XN” que contiene una salida válida del algoritmo Punycode (como se define en RFC 3492, Sección 6.3) a partir de la quinta posición y siguientes.
- *Personal al servicio de la Administración Pública*: Funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público.
- *Registro CAA (CAA records):* Registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (CAA). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (AC) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de CAA permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada de un *Certificado de autenticación de sitios web* para su nombre de dominio.

- *Responsable de la Oficina de Registro* (de aplicación exclusivamente para los *Certificados de sede electrónica*): Persona física nombrada por el representante de la Administración pública, organismo público o entidad de derecho público, bajo cuya responsabilidad se realizan las tareas asignadas a la *Oficina de Registro* con las obligaciones y responsabilidades asignadas en las presentes *Políticas y Prácticas de Certificación Particulares*.
- *Representante del Suscriptor*: es la persona física representante legal, o persona autorizada por éste, de la organización *Suscriptora* del *Certificado de autenticación de sitios web*, para la solicitud y uso de dicho *Certificado*.
- *Sede electrónica*: Dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.
- *Suscriptor*: Persona jurídica, órgano u organismo público destinatario de las actividades de la FNMT-RCM como *Prestador de Servicios de Confianza*, que suscribe los términos y condiciones del servicio. Bajo las presentas *Políticas de Certificación*, dicho servicio consiste en la expedición de *Certificados de autenticación de sitios web*. El *Suscriptor* se referencia en el campo *Sujeto* del *Certificado* y es el titular y responsable de su uso y posee el control exclusivo y la capacidad de decisión sobre el mismo.

1.6.2. Acrónimos

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

AC: Autoridad de Certificación

AR: Autoridad de Registro

ARL: Lista de Revocación de Autoridades de Certificación

CN: Nombre común (Common Name)

CRL: Lista de *Certificados* revocados

DN: Nombre distintivo (Distinguished Name)

DPC: Declaración de Prácticas de Certificación

ECDSA: Algoritmo de firma de curva elíptica (Elliptic Curve Digital Signature Algorithm)

eIDAS: Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

eIDAS2: Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital que modifica al eIDAS.

EV: Validación extendida (Extended Validation).

ETSI: European Telecommunications Standards Institute

FQDN: Fully-Qualified Domain Name

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

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

OID: Identificador de Objeto (Object IDentifier)

OV: Validación de Organización (Organizational Validation).

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

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

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

PKI: Infraestructura de clave pública (Public Key Infrastructure).

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

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

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

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

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

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

34. Estas prácticas de Certificación se estructuran de acuerdo a la RFC 3647 e incluyen todo el contenido requerido por dicha RFC.

35. La FNMT-RCM emite certificados de conformidad con la versión vigente de los "Requisitos básicos para la emisión y gestión de certificados de servidor TLS de confianza", definidos por CA/Browser Forum, disponibles en la dirección https://cabforum.org/baseline-requirements-documents/. Asimismo, para Certificados EV, cumple con la versión vigente de la "Guía para la expedición y gestión de Certificados de Validación Extendida (EV)" publicada por dicha entidad en https://cabforum.org/extended-validation/. En caso de cualquier inconsistencia entre esta PC/DPC y estos requisitos establecidos por CA/Browser Forum, prevalecerán estos últimos.

36. La FNMT-RCM mantiene sitios web de prueba que permiten a los proveedores de software validar la interoperabilidad de sus aplicaciones con *Certificados de Autenticación de Sitios Web* que encadenan su confianza hasta los certificados raíz de la FNMT-RCM. La FNMT-RCM mantiene sitios web diferentes que usan estos *Certificados* en distintos estados: i). activo, ii) revocado, y iii) Expirado

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

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

2.3. FRECUENCIA DE PUBLICACIÓN

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

39. Cualquier modificación en la *PC/DPC* será publicada de forma inmediata en la URL de acceso a las mismas.

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. DENOMINACIÓN

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

42. Adicionalmente, para los *Certificados EV,* la FNMT-RCM cumplirá con los requisitos establecidos en CA/Browser forum en su "Guía para la expedición y gestión de Certificados de Validación Extendida" y que pueden consultarse en la dirección https://cabforum.org/extended-validation/

3.1.1. Tipos de nombres

43. Los *Certificados* electrónicos de entidad final objeto de la presente *PC/DPC* contienen un nombre distintivo (*DN*) en el campo Subject Name, que se componen según se describe en la información relativa al perfil del Certificado (apartado 7.1 del presente documento). La FNMT-RCM cumple con los requisitos X.500, RFC 5280 y CA/Browser Forum (BRs and EVGs) a este respecto.

44. El campo Common Name define al titular de Certificado.

3.1.2. Significado de los nombres

45. Todos los nombres distintivos (*DN*) de los campos Subject Name son significativos. Los nombres en los certificados identifican respectivamente al sujeto y al emisor. 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).

46. La FNMT-RCM no emite *Certificados Wildcard* con políticas EV.

3.1.3. Seudónimos

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

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

48. 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

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

3.1.6. Reconocimiento y autenticación de marcas registradas

50. Los suscriptores no podrán solicitar *Certificados* con ningún contenido que infrinja los derechos de propiedad intelectual de un tercero.

51. 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

52. La FNMT-RCM realiza el proceso de validación de la información incluida en el *Certificado de autenticación de sitios web,* de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza" establecidos por el CA/Browser Forum, los cuales pueden consultarse en: https://cabforum.org/baseline-requirements-documents/

53. Adicionalmente, antes de expedir un *Certificado EV*, *Certificado SAN EV* o *Certificado de sede electrónica*, la FNMT-RCM asegura que toda la información relativa al suscriptor incluida en dichos *Certificados* es conforme a y se verifica de acuerdo a los requisitos definidos por CA/Browser Forum en su "Guía para la expedición y gestión de Certificados de Validación Extendida", (apartado 3.2) y que pueden consultarse en la dirección https://cabforum.org/extended-validation/.

54. La FNMT-RCM registra todas las confirmaciones realizadas en esta sección para los procesos periódicos de auditoría, tanto interna como independiente.

3.2.1. Métodos para probar la posesión de la clave privada

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

3.2.2. Autenticación de la identidad de la Organización

56. Esta sección contiene información acerca de los procesos que la FNMT-RCM lleva a cabo en las fases de identificación y autenticación de los solicitantes en la fase de registro. Toda la documentación aquí tratada será inspeccionada para evitar alteraciones o falsificaciones.

3.2.2.1 Identidad

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

58. Cuando el *Suscriptor* es una entidad privada, se verificará su existencia, dirección e identidad, que está legalmente reconocida, activa en ese momento e inscrita formalmente, mediante consulta directa de la AR de la FNMT-RCM al servicio que el Registro Mercantil dispone para este fin.

59. En el caso de entidades públicas, dicha verificación se realizará mediante consulta directa de la AR de la FNMT-RCM al inventario de entes del sector público de la Intervención General de la Administración del Estado, dependiente del Ministerio de Hacienda, o al Boletín Oficial correspondiente.

60. Si la naturaleza del *Suscriptor* fuera distinta de los dos casos anteriores, las verificaciones relativas a la existencia legal, dirección y la identidad se realizará mediante consulta directa al registro oficial correspondiente.

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

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

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

64. En el caso de que la solicitud corresponda a un certificado EV, la FNMT-RCM cumplirá con los requisitos establecidos por CA/Browser Forum en su "Guía para la expedición y gestión de Certificados de Validación Extendida", los cuales pueden consultarse en: https://cabforum.org/extended-validation/

3.2.2.2 Nombre comercial o marca registrada

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

66. Para el caso de los *Certificados EV*, se requiere una verificación de identidad exhaustiva según se define en la sección 3.2.2.3 de CA/Browser forum en su "Guía para la expedición y gestión de Certificados de Validación Extendida"

3.2.2.3 Verificación del país

67. El país se verificará utilizando cualquiera de los métodos indicados en la Sección 3.2.2.1

3.2.2.4 Validación de la autorización y control sobre el dominio

68. Para validar el nombre de domino (FQDN) de los Certificados de autenticación de sitios web, la FNMT-RCM utiliza el siguiente método descrito en el documento de CA/Browser Forum Baseline Requirements: "3.2.2.4.7 DNS Change". La FNMT-RCM seguirá un proceso documentado y mantendrá registros que indiquen el método empleado para cada emisión, incluyendo el número de versión de CA/Browser Forum Baseline Requirements usada para el proceso de validación. El resto de los métodos descritos en CA/Browser Forum Baseline Requirements no se emplea para la validación de dominios.

- 3.2.2.4.7 Cambio en DNS:

  Confirmar el control del Solicitante sobre el FQDN solicitado mediante la verificación de la presencia de un código aleatorio en un registro TXT o CAA de DNS para 1) un nombre de dominio; o 2) un nombre de dominio que tiene como prefijo una etiqueta que comienza con un carácter de subrayado. Se realiza de acuerdo al apartado 3.2.2.4.7 de los CA/Browser Forum Baseline Requirements, incluyendo la *Corroboración Multi-Perspectiva*.

  La FNMT-RCM proporcionará un código aleatorio exclusivo para la solicitud del certificado y no utilizará el código aleatorio después de 30 días.

69. La FNMT-RCM confirma que el Representante del Suscriptor posee el control sobre los nombres completos de los dominios o FQDN (siglas en inglés de Fully Qualified Domain Name) que son incorporados a los Certificados de autenticación de sitio web que expide. Para ello, la FNMT-RCM consulta, a través de la aplicación que registra las solicitudes de estos Certificados, la identidad del Representante del Suscriptor y el nombre del citado FQDN. A continuación, verifica que la solicitud proviene del contacto que tiene el control sobre dicho dominio (según los métodos definidos en el apartado anterior) o tiene autorización por parte de este. Adicionalmente se comprueba que la solicitud del Certificado ha sido realizada con posterioridad al alta en dichos registros.

70. Tal y como viene especificado en la CA/Browser Forum Baseline Requirements, la validación DNSSEC de vuelta hasta el anclaje de confianza raíz de la IANA se realiza en todas las consultas DNS asociadas a la validación o control del dominio por parte de la Perspectiva de Red Primaria. El servidor de resolución de DNS usado para todas las consultas DNS asociadas a la validación o control del dominio por parte de la Perspectiva de Red Primaria:

- realiza la validación DNSSEC usando el algoritmo definido en la RFC 4025 Sección 5; y
- es compatible con NSEC3 tal y como está definido en la RFC 5155; y
- es compatible con SHA-2 tal y como está definido en la RFC 4509 y la RFC 5702; y
- trata de manera adecuada las preocupaciones de seguridad enumeradas en la RFC 6840 Sección 4.

71. La FNMT- RCM no usa ninguna política local para desactivar la validación DNSSEC en ninguna consulta DNS asociada con la validación de la autorización o control sobre el dominio.

72. La validación DNSSEC hasta el anclaje de confianza raíz de la IANA se considera fuera de los requisitos de tipos de eventos registrados del apartado 5.4.1.

73. Adicionalmente, antes de la emisión de un Certificado de autenticación de sitios web, se verifica que el dominio a incluir en el Certificado es público (no es un dominio interno) y se consulta a registros púbicos para verificar que no es un dominio de alto riesgo (por ejemplo, el registro de Google creado para este fin, como es Safe Browsing site status).

3.2.2.5 Autenticación para una dirección IP

74. Bajo la presente *PC/DPC,* no se emiten certificados para identificar direcciones IP.

3.2.2.6 Validación de dominio wildcard

75. La *RA*, verificará que todo el espacio de nombres de dominio en los *Certificados Wildcard OV* es controlado legítimamente por el *Suscriptor*.

76. Si un *Certificado Wildcard* cayera dentro de la etiqueta inmediatamente a la izquierda de un sufijo público o un registro controlado, la FNMT_RCM rechazará la emisión de dicho *Certificado* a menos que el *Solicitante* demuestre el control legítimo de todo el espacio de nombres de dominio (p. ej., no se emitirá "*.co.uk" o "*.local", pero se puede emitir "*.example.com" a Example Co.). Para ello consultará la “Public Suffix List” disponible en https://publicsuffix.org/ y que se descargará periódicamente.

3.2.2.7 Fiabilidad de las fuentes de datos

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

3.2.2.8 Registro CAA

78. La FNMT-RCM comprueba si hay un Registro CAA para cada nombre de dominio que incluye en un Certificado de autenticación de sitios web emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento que dicha RFC establece para cualquier registro encontrado. Si existe dicho Registro CAA, se procesan los campos “issue”, “issuewild” e “iodef”. La FNMT-RCM no emitirá dicho Certificado si en los campos de emisor no aparece la etiqueta de la *Autoridad de Certificación* con identificador de dominio “fnmt.es” o si aparece una etiqueta marcada como crítica (critical flag) que no se

reconoce. Únicamente se permitirán los esquemas de la URL "mailto:" y "https:" para el campo "iodef". El solicitante deberá modificar los datos en el registro CAA de su dominio para que FNMT-RCM pueda emitir el certificado.

79. Una vez procesado el registro CAA, la FNMT-RCM emitirá el certificado en un plazo inferior a 8 horas.

80. La FNMT-RCM documentará con suficiente detalle cualquier problema relacionado con el registro CAA que imposibilite la emisión, por si fuera necesario proporcionar la información a CA/Browser Forum.

3.2.2.8.1 Validación DNSSEC de Registros CAA

81. Tal y como viene especificado en la CA/Browser Forum Baseline Requirements, la validación DNSSEC de vuelta hasta el anclaje de confianza raíz de la IANA se realiza en todas las consultas DNS asociadas a las comprobaciones de registros CAA por parte de la Perspectiva de Red Primaria. El servidor de resolución de DNS usado para todas las consultas DNS asociadas a la a las comprobaciones de registros CAA por parte de la Perspectiva de Red Primaria:

- realiza la validación DNSSEC usando el algoritmo definido en la RFC 4025 Sección 5; y
- es compatible con NSEC3 tal y como está definido en la RFC 5155; y
- es compatible con SHA-2 tal y como está definido en la RFC 4509 y la RFC 5702; y
- trata de manera adecuada las preocupaciones de seguridad enumeradas en la RFC 6840 Sección 4.

82. La FNMT-RCM no usa ninguna política local para desactivar la validación DNSSEC en ninguna consulta DNS asociada con las comprobaciones de registros CAA.

83. La FNMT-RCM no tratará los errores de validación DNSSEC detectados por la Perspectiva de Red Primaria como permiso para la emisión.

84. Estas validaciones DNSSEC se consideran fuera del ámbito de las auditorías internas del apartado 8.7.

3.2.2.9 Corroboración de Emisión Multi-Perspectiva

85. La FNMT-RCM comprueba si hay un Registro CAA para cada nombre de dominio que incluye en un Certificado de autenticación de sitios web emitido,

86. La FNMT-RCM emplea el mismo conjunto de Perspectivas de Red durante la realización de la Corroboración de Emisión Multi-Perspectiva para los requisitos de 1) Autorización o Control de Dominio y 2) Chequeos de Registros CAA.

87. El conjunto de respuestas sobre las Perspectivas de Red en las que se confía proporcionan a la FNMT-RCM la información necesaria para poder evaluar correctamente:

- La presencia del valor esperado del código aleatorio, tal y como viene especificado por el método de validación de confianza definido en el apartado 3.2.2.4 de esta *CP/DPC; y*

- La autoridad de la FNMT-RCM para emitir para el dominio solicitado, tal y como se indica en el apartado 3.2.2.8

88. En una Perspectiva de Red se pueden emplear servidores DNS para la resolución de nombres de dominio que no estén en la misma ubicación, pero pertenezcan a la misma región del Registro Regional de Internet de la Perspectiva de Red. Además, al menos habrá 500 km de distancia entre estados, provincias o países donde se encuentren dos servidores DNS que participen en la corroboración.

89. Para la Perspectiva Remota de Red la FNMT-RCM confía en redes que implementan medidas de mitigación ante incidentes de enrutamiento BGP.

90. Este método está implementado de acuerdo con CA-Browser Forum TLS Baseline Requirements, apartado 3.2.2.9.

3.2.3. Autenticación de la identidad de la persona física solicitante

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

3.2.4. Información no verificada del Suscriptor

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

3.2.5. Validación de la capacidad de representación

93. La AR de la FNMT-RCM verifica que el *Solicitante* tiene suficiente capacidad de representación mediante la firma electrónica del formulario de solicitud, según se describe en el apartado 3.2.3 de la presente *PC/DPC*, aceptando el uso de un *Certificado* cualificado de representante de administrador único o solidario de la persona jurídica suscriptora o un *Certificado* cualificado de *Personal al servicio de la Administración Pública*, para cuya expedición ha sido acreditada la capacidad de representación.

94. Cuando el citado formulario se firma mediante un *Certificado* cualificado diferente de los mencionados en el apartado anterior, la AR de la FNMT-RCM comprueba la facultad de representación del firmante de la solicitud mediante consulta a registros oficiales (Registro Mercantil, Boletines Oficiales, etc. en función de la naturaleza de la representación). Si del resultado de estas consultas no se obtuvieran evidencias de representación suficiente, la AR de la FNMT-RCM se pondrá en contacto con el *Suscriptor* para recabar dichas evidencias.

95. Para las solicitudes de certificados EV, la FNMT-RCM cumplirá con los requisitos definidos por la entidad CA/Browser forum en su "Guía para la expedición y gestión de Certificados de Validación Extendida" (apartados 3.2.2.8 y 3.2.2.11).

3.2.6. Criterios de interoperación

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

3.3.1. Identificación y autenticación para renovación rutinaria de claves

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

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

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

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

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

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. Quién puede solicitar un Certificado

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

101. Adicionalmente, para *Certificados EV*, la FNMT-RCM cumplirá los requisitos de la sección 3.2 de la "Guía para la emisión y gestión de Certificados de Validación Extendida" establecidos por CA/Browser Forum.

4.1.2. Proceso de registro y responsabilidades

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

103. El proceso de registro incluye las siguientes fases:

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

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

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

106. El apartado 9.6 "Obligaciones y garantías" del presente documento establece las responsabilidades de las partes en este proceso.

4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

4.2.1. Realización de las funciones de identificación y autenticación

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

- Verificación de que el solicitante está autorizado para obtener el certificado.
- Confirmación de la identidad del solicitante y, si aplica, de la organización asociada, incluyendo verificación de nombre, dirección y DBA/nombre comercial según las secciones 3.2.2.1 y 3.2.2.2.
- Obtención de la clave pública y verificación de la posesión de la clave privada generada por el solicitante.
- Verificación de que cualquier agente que presente la solicitud está debidamente autorizado.

108. La FNMT-RCM comprobará la veracidad de los datos incluidos en la solicitud y, en su caso, la capacidad del *Representante* a través de las verificaciones correspondientes y conservando las evidencias de validación oportunas.

109. La *Firma Electrónica* generada para la suscripción del contrato será verificada por la FNMT-RCM para asegurar su autenticidad e integridad.

110. La información del Solicitante deberá incluir, aunque no estará limitada a, al menos un Fully-Qualified Domain Name (FQDN) para ser incluida en la extensión subjectAltName del *Certificado.*

111. El empleo de los datos o la documentación de validación previa, obtenidos de una fuente de las especificadas en la sección 3.2, no se puede utilizar más de 398 días después de la validación de dichos datos o documentación. En ningún caso se podrán reutilizar validaciones anteriores que excedan dicho plazo.

112. El empleo de los chequeos de dominio previamente completados (validaciones de DNS) obtenidos de unas fuentes y métodos especificadas en la sección 3.2.24, no se puede utilizar más de 200 días después de la validación de dichos datos o documentación. En ningún caso se podrán reutilizar validaciones anteriores que excedan dicho plazo.

4.2.2. Aprobación o rechazo de la solicitud del certificado

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

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

115. La FNMT-RCM mantiene una base de datos interna de todos los *Certificados* revocados y de todas las solicitudes de *Certificados* rechazadas previamente debido a sospecha de phishing u otro uso fraudulento. Esta información es tenida en cuenta para identificar posteriores solicitudes de *Certificados* sospechosos antes de proceder a la aprobación de la expedición de los mismos.

116. Adicionalmente, FNMT-RCM desarrolla, mantiene e implementa procedimientos documentados que identifican y requieren actividad de verificación adicional para las solicitudes de *Certificados* de alto riesgo antes de la aprobación de la expedición del *Certificado*, según sea razonablemente necesario para garantizar que dichas solicitudes se verifican adecuadamente según estos requisitos.

117. Si alguna de estas validaciones no ha podido ser confirmada, la FNMT-RCM rechazará la solicitud del *Certificado*, reservándose el derecho de no revelar los motivos de dicha denegación. El *Representante del Suscriptor* cuya solicitud haya sido rechazada podrá volver a solicitarlo posteriormente.

118. Cualquier solicitud de *Certificado OV* o *Certificado EV* será tramitada por personal de la FNMT-RCM con el rol de confianza para tal efecto. El sistema de aprobación de expedición de los *Certificados EV* requiere de la acción de al menos dos personas pertenecientes a la AR de la FNMT-RCM con rol de confianza, uno para validar la solicitud y otro para aprobarla.

119. Adicionalmente, la FNMT-RCM comprueba si hay un *Registro CAA* para cada nombre de dominio que incluye en un *Certificado de autenticación de sitios web* emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento que dicha RFC establece para cualquier registro encontrado. Si existe dicho *Registro CAA*, no

emitirá dicho *Certificado* a menos que determine que la solicitud del *Certificado* es consistente con el conjunto de registro de recursos AAC aplicable. El identificador de dominio reconocido como propio asociado a la *Autoridad de Certificación* de la FNMT se ha establecido en "fnmt.es".

120. La FNMT-RCM no emite *Certificados* que contienen Internal Names.

4.2.3. Tiempo en procesar la solicitud

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

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

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. Acciones de la AC durante la emisión

123. Una vez aprobada la solicitud del *Certificado* por parte de la AR de la FNMT-RCM, el sistema de generación de certificados cuenta con una serie de controles, previos a la emisión del certificado que verifican el cumplimiento de requisitos de la RFC 5280 y CA/Browser Forum (BRs and EVGs). Tras esta verificación se procede a expedir el *Certificado* conforme al perfil aprobado para cada tipo de *Certificado*.

124. Así mismo, la FNMT-RCM monitoriza periódicamente posibles desviaciones en los certificados emitidos.

125. La FNMT-RCM emplea herramientas de linting sobre los certificados, tanto en procesos de pre-emisión como de post-emisión, para prevenir errores y/o reducir emisiones incorrectas, utilizando pkimetal entre otras

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

127. La emisión de Certificados por parte de una AC Raíz requiere de una persona con un rol de confianza designado por la FNMT-RCM que ejecute de forma deliberada una orden directa para que la AC Raíz realice la operación de firma del certificado.

4.3.2. Notificación de emisión de certificado

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

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. Proceso de aceptación

129. La aceptación del Certificado se entiende realizada cuando el *Suscriptor* o su Representante:

- Acepta las condiciones de uso y expresa su voluntad de obtener el *Certificado*, como requisitos necesarios para la generación del mismo, durante el proceso de solicitud, expresando formalmente su voluntad de obtener el Certificado y aceptando los términos asociados a la correspondiente Política de Certificación; y
- Descarga y/o instala el Certificado, haciéndolo técnicamente disponible para su uso.

4.4.2. Publicación del certificado por la AC

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

4.4.3. Notificación de la emisión a otras entidades

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

4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

4.5.1. Clave privada del suscriptor y uso del certificado

132. La FNMT-RCM no genera ni almacena las *Claves Privadas* asociadas a los *Certificados* expedidos bajo la presente *Política de Certificación*.

133. Corresponde la condición de custodio y el control de las claves del *Certificado* al *Responsable de Operaciones de Registro* en el caso del *Certificado de sede electrónica* y, para el resto de *Certificados de autenticación de sitio web*, a los *Representantes del Suscriptor* que hayan acreditado tener el control sobre el nombre del dominio a incluir en el *Certificado*.

134. Por tanto, la *Clave Privada* asociada a la *Clave Pública* estará bajo la responsabilidad de dicho custodio y actuará como representante de la Entidad que tiene la titularidad, gestión y administración de la dirección electrónica correspondiente.

135. El Suscriptor garantizará que certificado deberá instalarse únicamente en los servidores o sistemas accesibles mediante los nombres incluidos en el campo subjectAltName del Certificado, y utilizarse exclusivamente para los fines permitidos y conforme a esta PC/DPC, al acuerdo firmado con la FNMT-RCM y a la normativa aplicable.

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

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

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

4.6. RENOVACIÓN DEL CERTIFICADO

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

139. Bajo las presentes *Políticas de Certificación*, la FNMT-RCM no renueva *Certificados* manteniendo la *Clave pública* del mismo, sino que, en todo caso, la renovación de *Certificados* se realiza renovando las *Claves criptográficas*, según se define en el apartado "4.7 Renovación con regeneración de las claves del certificado" del presente documento.

4.6.1. Circunstancias para la renovación del certificado

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

4.6.2. Quién puede solicitar la renovación del certificado

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

4.6.3. Procesamiento de solicitudes de renovación del certificado

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

4.6.4. Notificación de la renovación del certificado

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

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

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

4.6.6. Publicación del certificado renovado

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

4.6.7. Notificación de la renovación del certificado a otras entidades

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

4.7. RENOVACIÓN CON REGENERACIÓN DE LAS CLAVES DEL CERTIFICADO

147. La renovación con regeneración de claves de los *Certificados de autenticación de sitios web* se realiza siempre emitiendo nuevas claves públicas y privadas, siguiendo el mismo proceso que el descrito para la emisión de un *Certificado* nuevo.

4.7.1. Circunstancias para la renovación con regeneración de claves

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

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

4.7.2. Quién puede solicitar la renovación con regeneración de claves

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

4.7.3. Procesamiento de solicitudes de renovación con regeneración de claves

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

4.7.4. Notificación de la renovación con regeneración de claves

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

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

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

4.7.6. Publicación del certificado renovado

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

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

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

4.8. MODIFICACIÓN DEL CERTIFICADO

155. 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

156. No se estipula la modificación.

4.8.2. Quién puede solicitar la modificación del certificado

157. No se estipula la modificación.

4.8.3. Procesamiento de solicitudes de modificación del certificado

158. No se estipula la modificación.

4.8.4. Notificación de la modificación del certificado

159. No se estipula la modificación.

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

160. No se estipula la modificación.

4.8.6. Publicación del certificado modificado

161. No se estipula la modificación.

4.8.7. Notificación de la modificación del certificado a otras entidades

162. No se estipula la modificación.

4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO

163. Los *Certificados de autenticación de sitios web* emitidos por la FNMT-RCM quedarán sin efecto en los siguientes casos:

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

b) Cese en la actividad como *Prestador de Servicios de Confianza* de la FNMT-RCM, salvo que, previo consentimiento expreso del *Suscriptor*, los *Certificados* expedidos por la FNMT-RCM hayan sido transferidos a otro *Prestador de Servicios de Confianza*.

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

c) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.

164. Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán desde la fecha en que la FNMT-RCM tenga conocimiento cierto de cualquiera de los hechos determinantes y así lo haga constar en su *Servicio de información y consulta sobre el estado de los certificados*.

165. La FNMT-RCM pone a disposición de los *Suscriptores*, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-

RCM https://www.sede.fnmt.gob.es/, con instrucciones claras, para permitirles reportar cualquier asunto relacionado con este tipo de Certificados, en cuanto a un supuesto compromiso de Clave Privada, uso indebido de los Certificados u otros tipos de fraude, compromiso, mal uso o conducta inapropiada.

166. La FNMT-RCM, como *Prestador de Servicios de Confianza,* se reserva el derecho de no expedir o revocar este tipo de *Certificados* si el *Suscriptor* que tiene el control del nombre de dominio del sitio web incluido en el *Certificado* no hace un uso adecuado del mismo, conculcando derechos de propiedad industrial o intelectual de terceros sobre las aplicaciones, sitios web o *Sedes electrónicas* que se desean proteger con tales *Certificados*, o su uso se presta a engaño o confusión sobre la titularidad de tales aplicaciones, sitios web o *Sedes electrónicas* y, por tanto, de sus contenidos. En especial, tal reserva de derechos se podrá ejecutar por la FNMT-RCM cuando en la utilización de tales *Certificados* se atente contra los siguientes principios:

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

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

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

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

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

4.9.1. Circunstancias para la revocación

4.9.1.1 Causas de revocación de un Certificado de entidad final

168. Adicionalmente a lo previsto en el apartado anterior, la FNMT-RCM procederá a la revocación de un *Certificado de autenticación de sitios we*b cuando concurra cualquiera de las circunstancias que se describen a continuación.

169. Las obligaciones de revocación se ejecutarán conforme a los plazos establecidos en las presentes prácticas, sin perjuicio de los periodos máximos establecidos por los requisitos del CA/Browser Forum.

170. Asimismo, la FNMT-RCM incluirá en la lista de revocación el código CRLReason correspondiente conforme a la sección 7.2.2 CA/Browser Forum, en función del motivo aplicable

171. La FNMT-RCM revocará el Certificado sin demora injustificada y, en todo caso, dentro de un plazo máximo de veinticuatro (24) horas desde la recepción, verificación o identificación de cualquiera de los siguientes eventos:

a) La solicitud de revocación por parte del Suscriptor o de una persona autorizada, aunque no se especifique un motivo concreto. Sin perjuicio de lo anterior, dicha solicitud de revocación podrá originarse entre otros, por los siguientes supuestos:

- La pérdida del soporte del *Certificado*.
- La utilización por un tercero de la *Clave Privada* asociada al *Certificado*.
- La violación o puesta en peligro del secreto de la *Clave Privada* asociada al *Certificado*, incluyendo cualquier evidencia razonable de compromiso criptográfico o técnico.
- No aceptación de las nuevas condiciones que puedan suponer la emisión de nuevas *Declaraciones de Prácticas de Certificación*, durante el periodo de un (1) mes tras su publicación

b) Resolución judicial o administrativa que así lo ordene.

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

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

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

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

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

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

i) Uso del Certificado con el propósito de generar dudas a los usuarios sobre la procedencia de los productos o servicios ofertados, incluyendo específicamente el supuesto en que un Certificado tipo *Wildcard* sea utilizado para autenticar dominios subordinados fraudulentos. Para ello, se seguirán los criterios sobre actividad infractora de las normas sobre consumidores y usuarios, comercio, competencia y publicidad.

j) Solicitar para el Sujeto del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que el Suscriptor no sea titular, licenciatario o usuario autorizado.

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

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

m) Incumplimiento de los requisitos definidos por los esquemas de auditorías a los que se somete la *Autoridad de Certificación* que expide los *Certificados* cubiertos por la presente *PC/DPC*, con especial atención a los de algoritmia y tamaños de clave, que supongan un riesgo inaceptable por parte de las partes que confían en estos *Certificados*.

n) Compromiso confirmado de la Clave Privada del Suscriptor correspondiente a la clave pública del certificado, o conocimiento de un método demostrado o probado que pueda exponer la Clave Privada del Suscriptor a riesgo, incluyendo defectos en el método de generación de la clave.

o) Notificación de que la solicitud de certificado original no fue autorizada y que no concede la autorización de forma retroactiva.

p) Evidencia de que la validación de la autorización o el control del dominio para cualquier Fully-Qualified Domain Name (FQDN) incluido en el certificado no debe ser confiable

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

173. La FNMT-RCM revocará el Certificado sin demora injustificada y, en todo caso, dentro en un plazo máximo de cinco (5) días, a partir de la verificación del hecho causante, cuando se produzca cualquiera de las siguientes situaciones:

q) El certificado ya no cumple los requisitos criptográficos establecidos en las secciones 6.1.5 y 6.1.6 de los CA/B Forum Baseline Requirements.

r) Incumplimiento sustancial por parte del Suscriptor de los términos del Acuerdo de Suscriptor, Términos de Uso u obligaciones derivadas de esta PC/DPC, que no implique riesgo inmediato de compromiso de clave o fraude.

s) El derecho de la FNMT-RCM a emitir Certificado de autenticación de sitios web finaliza, es suspendido o revocado, salvo que exista garantía de continuidad de servicios OCSP/CRL.

t) Factores externos fuera del control del Suscriptor o de la FNMT-RCM (incluyendo fuerza mayor, fallo técnico grave o brecha de seguridad) impiden garantizar el uso seguro del certificado y existe riesgo para terceros, sin implicar compromiso directo de la clave privada.

174. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:

- Que la revocación le haya sido solicitada por el *Representante del Suscriptor* siguiendo el procedimiento establecido para este tipo de *Certificados.*
- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*.
- Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
- Que en las causas c) a g) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.

175. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos o el *Certificado*, las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.

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

4.9.1.2 Causas de revocación de un Certificado de CA subordinada

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

a) La CA subordinada solicita la revocación por escrito;

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

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

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

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

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

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

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

i) La *PC/DPC* de la CA emisora requiere la revocación.

4.9.2. Quién puede solicitar la revocación

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

179. La revocación de un *Certificado de autenticación de sitios web* solamente podrá ser solicitada por la persona con facultades de representación del *Suscriptor* al que se ha expedido el *Certificado*.

180. En el caso de un *Certificado de Sede electrónica*, la FNMT-RCM presumirá la competencia y capacidad del *Solicitante* cuando se trate del *Responsable de Operaciones de Registro* correspondiente. Adicionalmente, estarán legitimados para solicitar la revocación de dicho *Certificado*:

- El órgano directivo, organismo o entidad pública *Suscriptora* del *Certificado* o persona en quien delegue.
- La *Oficina de Registro*, —a través de su responsable— que esté designada a tal efecto, por la Administración, organismo o entidad de derecho público, *Suscriptora* del

Certificado a revocar, cuando detecte que alguno de los datos consignados en el *Certificado*

- es incorrecto, inexacto o haya variado respecto a lo consignado en el *Certificado,* o
- la persona física, custodio del *Certificado,* no se corresponda con el responsable máximo o designado para la gestión y administración de la dirección electrónica consignada en el *Certificado* objeto de la revocación

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

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

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

4.9.3. Procedimiento de solicitud de la revocación

183. Existe un servicio de atención telefónica, en horario 24x7, en los teléfonos 917406848 y 913878337, al que se pueden dirigir las solicitudes de revocación de *Certificados de autenticación de sitios web*. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.

184. Adicionalmente, es posible dirigir la solicitud de revocación al Área de Registro de la FNMT-RCM, siguiendo el siguiente procedimiento:

1. Solicitud del *Suscriptor*

   El *Representante del Suscriptor* enviará a la FNMT-RCM el formulario de solicitud de revocación, cumplimentado y firmado electrónicamente con alguno de los *Certificados* admitidos para la solicitud y por los canales electrónicos habilitados por esta Entidad.

2. Tramitación de la solicitud por la FNMT-RCM

   El registrador de la FNMT-RCM recibirá el contrato de revocación y realizará las mismas comprobaciones relativas a la identidad y capacidad del *Representante del Suscriptor* que para el caso de la solicitud de expedición y, si procediera, tramitará la revocación del *Certificado*.

185. En el caso de un *Certificado de Sede electrónica*, la FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración para solicitar la revocación de este tipo de *Certificados*, cuyo procedimiento es el siguiente:

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

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

2. Comparecencia y documentación.

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

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

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

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

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

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

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

186. Si la persona solicitante no puede aportar los datos requeridos o se determina que no está capacitada para solicitar la revocación, la solicitud de revocación será desestimada.

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

4.9.4. Periodo de gracia de la solicitud de revocación

188. 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

189. En de las 24 horas posteriores a la recepción de un *CPR*, la FNMT-RCM investigará los hechos y circunstancias relacionados y proporcionará un informe preliminar tanto al Suscriptor como a la entidad que lo presentó.

190. Después de revisar los hechos y circunstancias, la CA trabajará con el *Suscriptor* y cualquier entidad que genere un *CPR* u otro aviso relacionado con la revocación, para establecer si el *Certificado* será revocado o no y, de ser así, la fecha en la que la CA lo revocará. El período desde la recepción del *CPR* o el aviso relacionado con la revocación hasta la revocación publicada no excederá el plazo establecido en la sección 4.9.1.1.

191. La fecha seleccionada por la CA considerará los siguientes criterios:

1. La naturaleza del presunto problema (alcance, contexto, gravedad, magnitud, riesgo de daño);

2. Las consecuencias de la revocación (impactos directos y colaterales a los Suscriptores y Partes que Confían);

3. El número de CPR recibidos sobre un Certificado o Suscriptor en particular;

4. La entidad que presenta la queja ; y

5. Legislación relevante.

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

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

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

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

4.9.7. Frecuencia de generación de CRLs

194. 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.

195. Las *CRL* de los certificados de *Autoridad* se emiten al menos cada seis (6) meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de seis (6) meses.

196. La *Autoridad de Certificación* continuará emitiendo CRLs de manera continua hasta que se cumpla alguna de las siguientes condiciones:

- Todos los certificados de CA subordinadas que contengan la misma Clave Pública de Sujeto hayan expirado o sido revocados; o
- La Clave Privada correspondiente de la CA subordinada haya sido destruida.

197. La FNMT-RCM garantizará el cumplimiento de los Requisitos Básicos (y de Validación Extendida, para certificados EV) del CA/Browser Forum.

4.9.8. Periodo máximo de latencia de las CRLs

198. 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

199. 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.

200. 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. Para cada petición válida, se emitirá una respuesta de OCSP informando acerca del estado actual de los certificados solicitados.
- Cada 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.
- Las respuestas OCSP son firmadas por un certificado OCSP Responder separado, que a su vez esté firmado por la AC emisora, y que contiene la extensión id-pkix-ocsp-nocheck según RFC6960.

201. Las respuestas OCSP para los certificados de suscriptor tendrán un intervalo de validez mayor o igual a ocho (8) horas y menor o igual a diez (10) días. El intervalo de validez de una respuesta OCSP es la diferencia de tiempo entre los campos thisUpdate y nextUpdate, ambos inclusive. A efectos del cálculo de diferencias, una diferencia de 3600 segundos será igual a una hora, y una diferencia de 86400 segundos será igual a un día, sin tener en cuenta los segundos intercalares.

202. Para el estado de un certificado de suscriptor o su precertificado correspondiente:

- La FNMT-RCM garantiza que una respuesta OCSP autoritativa estará disponible en un plazo máximo de quince (15) minutos después de que el certificado o precertificado se publique por primera vez o se ponga a disposición de otro modo.
- Para las respuestas OCSP con intervalos de validez inferiores a dieciséis (16) horas, FNMT-RCM proporcionará una respuesta OCSP actualizada antes de la mitad del período de validez anterior a la próxima actualización.

203. Para certificados de AC subordinadas, se proporcionará una respuesta OCSP actualizada al menos una vez cada 12 meses y dentro de 24 horas tras la revocación del certificado.

204. Si el OCSP responder recibe una solicitud de un número de serie no asignado (unassigned), no deberá emitir una respuesta con estado good.

205. Los OCSP responders soportan el método HTTP GET, conforme a RFC 6960 y RFC 5019. Opcionalmente, pueden procesar la extensión Nonce de acuerdo con RFC8954

4.9.10. Requisitos de comprobación en línea de la revocación

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

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

4.9.11. Otras formas de aviso de revocación disponibles

207. No definidas.

4.9.12. Requisitos especiales de revocación de claves comprometidas

208. 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.

209. 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.

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

4.9.13. Circunstancias para la suspensión

211. No se contempla la suspensión de certificados.

4.9.14. Quién puede solicitar la suspensión

212. No se contempla la suspensión de certificados.

4.9.15. Procedimiento para la petición de la suspensión

213. No se contempla la suspensión de certificados.

4.9.16. Límites sobre el periodo de suspensión

214. No se contempla la suspensión de certificados.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

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

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

217. La FNMT-RCM opera y mantiene sus capacidades de mantenimiento de sus CRL y servicio OCSP con recursos suficientes para proporcionar un tiempo de respuesta máximo de diez segundos bajo condiciones normales de operación.

218. El acceso a estos servicios de información es:

- Listas de certificados revocados:

  AC RAIZ FNMT-RCM "SERVIDORES SEGUROS":

  http://www.cert.fnmt.es/crls/ARLSERVIDORESSEGUROS.crl

  CA Subordinada "SERVIDORES SEGUROS TIPO 1" (*EV Certificates)*:

  http://www.cert.fnmt.es/crlsservseguros/CRLT1.crl

  CA Subordinada "SERVIDORES SEGUROS TIPO 2" (*OV Certificates)*:

  http://www.cert.fnmt.es/crlsservseguros/CRLT2.crl

  AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R:

  http://www.cert.fnmt.es/crls/ARLFNMTRCMSERVIDORESSEGUROSG2R.crl

  CA Subordinada "SERVIDORES SEGUROS TIPO 1 G2" (*EV Certificates)*:

  http://www.cert.fnmt.es/crlsservseguros/CRLT1G2E.crl

  CA Subordinada "SERVIDORES SEGUROS TIPO 2 G2" (*OV Certificates)*:

http://www.cert.fnmt.es/crlsservseguros/CRLT2G2E.crl

CA Subordinada "SERVIDORES SEGUROS TIPO 2 G2R" (*OV Certificates)*:

http://www.cert.fnmt.es/crlsservseguros/CRLT2G2R.crl

- Servicio de verificación del estado de certificados (OCSP):

  AC RAIZ FNMT-RCM "SERVIDORES SEGUROS".

  http://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder

  CA Subordinada "SERVIDORES SEGUROS TIPO 1" (*EV Certificates)*.

  http://ocspfnmtss1.cert.fnmt.es/ocspss1/OcspResponder

  CA Subordinada "SERVIDORES SEGUROS TIPO 2" (*OV Certificates)*.

  http://ocspfnmtss2.cert.fnmt.es/ocspss2/OcspResponder

  CA Subordinada "SERVIDORES SEGUROS TIPO 1 G2" (*EV Certificates)*.

  http://ocspfnmtss1.cert.fnmt.es/ocspss1g2e/OcspResponder

  CA Subordinada "SERVIDORES SEGUROS TIPO 2 G2" (*OV Certificates)*.

  http://ocspfnmtss2.cert.fnmt.es/ocspss2/OcspResponder

  CA Subordinada "SERVIDORES SEGUROS TIPO 2 G2R" (*OV Certificates)*.

  http://ocspfnmtss2.cert.fnmt.es/ocspss2g2r/OcspResponder

4.10.1. Características operativas

219. Las entradas de revocaciones en una CRL o respuesta OCSP incluirán todos los certificados revocados, incluidos aquellos que hayan expirado. En ningún caso se eliminarán entradas de revocación antes de la fecha de expiración del certificado.

4.10.2. Disponibilidad del servicio

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

221. La FNMT-RCM opera y mantiene su capacidad CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de funcionamiento.

222. En el caso de indisponibilidad del servicio por operaciones de mantenimiento, la FNMT-RCM notificará esta circunstancia en la dirección http://www.ceres.fnmt.es, si es posible con al menos cuarenta y ocho (48) horas de antelación, y tratará de solventarla en un periodo no superior a veinticuatro (24) horas.

4.10.3. Características opcionales

223. No estipuladas.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

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

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. Prácticas y políticas de custodia y recuperación de claves

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

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

226. No estipulado.

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

227. 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.

228. 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.

229. 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.

230. A continuación y tomando como modelo de trabajo el documento RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 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 los requisitos CAB Forum “Network Security and Certification System” 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

231. 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.

232. 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

233. 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

234. 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.

235. 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

236. 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.

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

5.1.2.2 Controles físicos de entrada

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

239. 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.

240. 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

241. 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

242. 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

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

5.1.3. Electricidad y Aire Acondicionado

244. 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.

245. 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*.

246. 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

247. 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

248. 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

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

5.1.6. Almacenamiento de Soportes

250. 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

251. La FNMT-RCM dispone de 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

252. 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

253. La FNMT-RCM custodia soportes de copia de seguridad y archivado en un almacén alternativo seguro propio, independiente del centro principal y a suficiente distancia para prevenir daños en caso de desastre.

254. Para acceder a la retirada o inclusión de nuevos soportes se requiere al menos tres personas autorizadas.

5.2. CONTROLES DE PROCEDIMIENTO

255. 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.

256. 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.

257. 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.

258. 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.

259. 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.

260. 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[3] 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

261. 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.

262. 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.

263. La lista de personal designado como Rol de Confianza se mantiene y se revisa cada vez que hay un cambio en los roles o con periodicidad máxima anual.

5.2.2. Número de personas por tarea

264. 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".

265. Las claves privadas de FNMT son respaldadas, almacenadas y recuperadas exclusivamente por personal con rol de confianza, con al menos control dual y en un ambiente físicamente seguro.

5.2.3. Identificación y autenticación para cada rol

266. 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".

[3] 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.

5.2.4. Roles que requieren segregación de funciones

267. Las funciones desempeñadas se corresponden con los Roles de Confianza definidos en el apartado 5.2.1. Cada persona designada asume un único rol.

268. En el caso de certificados EV, una vez se haya realizado la validación, un Especialista de Validación de la FNMT-RCM, distinto al que ha recopilado y revisado los documentos de la solicitud, verificará el conjunto de la información y aprobará su emisión.

5.3. CONTROLES DE PERSONAL

269. 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.

270. 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.

271. 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.

272. 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.

273. 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.

274. 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.

275. 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.

276. 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.

277. 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.

278. 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

279. 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, que verificará la identidad e integridad de los candidatos, de forma que el perfil profesional del empleado sea el más adecuado posible a las características propias de las tareas a desarrollar. La confiabilidad e idoneidad de los roles de confianza asignados se revisan periódicamente.

280. 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.

281. 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

282. 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

283. 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".

284. Para el personal que realiza tareas de verificación de información, la formación anual cubrirá conocimientos básicos de Infraestructura de clave pública, políticas y procedimientos de autenticación y verificación (incluida la Política de certificados y / o Declaración de prácticas de certificación de la FNMT), amenazas comunes al proceso de verificación de información (incluido el phishing y otras tácticas de ingeniería social), los "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" y los "EV SSL Certificate Guidelines" establecidos por la entidad CA/Browser Forum.

285. 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.

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

287. La FNMT-RCM requiere que todos los Especialistas en Validación superen un examen sobre los requisitos de verificación de información descritos en "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

5.3.4. Requisitos y frecuencia de actuación formativa

288. 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*. Estos requisitos son revisados al menos una vez al año.

5.3.5. Secuencia y frecuencia de rotación laboral

289. No estipulado.

5.3.6. Sanciones por acciones no autorizadas

290. 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.

291. 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 62, las Faltas y Sanciones del referido Convenio Colectivo:

> *"Serán faltas muy graves:*
>
> *...*
>
> *9. La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso los trabajadores por razón de su cargo o función.*
>
> *10. La negligencia en la custodia de secretos oficiales, declarados así por la Ley o clasificados como tales, que sea causa de su publicación o que provoque su difusión o conocimiento indebido.*
>
> *..."*

292. 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.

293. 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

294. 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).

295. 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.

296. En el caso de que se asignase a un tercero independiente para realizar tareas de un Rol de Confianza del servicio de certificación, la FNMT-RCM verificará que el personal involucrado cumpla con los requisitos de capacitación y habilidades de la sección 5.3.3 y los requisitos de retención de documentos y registro de eventos de la sección 5.4.1

5.3.7.1 Requisitos de contratación de terceros

297. 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. Para los casos en que no se aplique la LCSP, la FNMT-RCM empleará sus Instrucciones Internas de Contratación (IIC).

5.3.8. Suministro de documentación al personal

298. 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, *Políticas y Prácticas 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.

299. 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.

300. 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.

301. 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

302. 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.

303. 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

304. 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.

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

306. 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

307. 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”.

308. 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.

309. La 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 "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" y en esta *PC/DPC*;
3. Aprobación y rechazo de las solicitudes de certificados;
4. Emisión de certificados;
5. Generación de entradas en las CRLs y OCSP; e
6. Intentos de Corroboración de Emisión Multi-Perspectiva desde cada Perspectiva de Red, con identificador de la perspectiva, nombre de dominio, resultado de cada intento y resultado del quorum de la corroboración.

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

5.4.1.1 Registro o Log de actividades con Firewall y enrutadores

310. El registro de las actividades del Firewall y los routers (enrutadores) incluyen:

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

311. 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

312. La FNMT-RCM conservará los registros por al menos 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

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

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

315. 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.

316. 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

317. 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. Sistemas de recolección de registros

318. Los eventos significativos generados por la 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

319. No se contempla.

5.4.8. Evaluación de vulnerabilidades

320. La FNMT-RCM dispone de un procedimiento de gestión de vulnerabilidades en el que se habla de la detección, registro y tratamiento de vulnerabilidades detectadas en el sistema.

321. Se definen y establecen las responsabilidades asociadas con la gestión de vulnerabilidades técnicas y se mantiene un inventario de activos con los recursos de la información actualizados. Asimismo, se realizan auditorías periódicas de los procedimientos emprendidos y se monitoriza y evalúa periódicamente la gestión de vulnerabilidades técnicas.

322. Se 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.

323. La FNMT-RCM realiza semanalmente un análisis de vulnerabilidades en sus sistemas y toma las medidas apropiadas. Adicionalmente se realiza un test anual de penetración y un análisis de riesgos anual para evaluar las amenazas y el daño potencial a los servicios de certificación.

5.5. ARCHIVADO DE REGISTROS

5.5.1. Tipos de registros archivados

324. 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.

325. 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.

326. 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

327. *Declaraciones de Políticas y Prácticas de Certificación* y su histórico.

5.5.2. Periodo de retención del archivo

328. El periodo de retención de los registros archivados no será inferior a 15 años tras la extinción de la vigencia del certificado asociado.

5.5.3. Protección del archivo

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

330. 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.

331. 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.

332. Se garantizará la confidencialidad de la información y quedará traza de los accesos realizados.

5.5.4. Procedimientos de copia de respaldo del archivo

333. 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

334. 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

335. 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.

336. 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

337. 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

338. 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. RECUPERACIÓN DE DESASTRES Y COMPROMISOS

5.7.1. Procedimientos de manejo de incidentes y compromisos

339. 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.

340. 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.

5.7.1.1. Planes de respuesta ante incidentes y recuperación ante desastres

341. La FNMT-RCM cuenta con un plan de respuesta ante incidentes y un plan de recuperación ante desastres.

342. La FNMT-RCM implementa, documenta y somete a pruebas anuales una serie de procedimientos de continuidad de negocio y de recuperación ante desastres para asegurar la integridad de sus servicios, notificar y proteger a proveedores de software, suscriptores y partes interesadas en caso de desastre o compromiso de seguridad. Estos planes y procedimientos se actualizan al menos una vez al año.

343. En el caso de fallo o desastre de los sistemas del *Prestador de Servicios de Confianza,* se pondrá en marcha un plan de respuesta y recuperación ante desastres, que contemple:

- Las condiciones para la activación del plan.
- Los procedimientos para la detección, registro y gestión del incidente.
- El tiempo estimado de recuperación.
- Los roles y responsabilidades de los participantes y la formación necesaria.
- 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.
- La protección de la infraestructura desde que se produce el desastre hasta que se restablece en un entorno seguro.
- El 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.

5.7.1.2. Plan de revocación masiva

344. La FNMT-RCM dispone de un plan de revocación masiva que se activará en el caso de que se requiera una revocación de un número sustancial de certificados en un plazo de tiempo corto debido a una causa común, requisito de cumplimiento o incidente de seguridad.

345. El plan define de manera clara, viable y comprensible para todos los participantes, una serie de procedimientos orientados a asegurar una respuesta rápida, consistente y fiable ante este tipo de escenarios. Consta de cuatro fases con un tiempo de realización estimado para cada subtarea: la comunicación con los clientes afectados, el reemplazo y revocación de los certificados y un análisis posterior para revisar la efectividad de la respuesta y retroalimentar el plan.

346. Los miembros participantes tienen asignados roles y responsabilidades que se especifican en el plan. Asimismo, para asegurarse de que el personal comprende sus roles, reciben una formación inicial y una formación anual de los procedimientos de respuesta.

347. La FNMT-RCM realiza un simulacro anual que sirve para revisar, actualizar y mejorar los procedimientos del plan.

348. El plan se revisa y actualiza como mínimo cada año, o cada vez se requiera al hacer el análisis de un incidente o simulacro.

5.7.2. Actuación ante recursos, software y/o datos corruptos

349. 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

350. 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.

351. Estudiar la necesidad de ejecutar el Plan de Cese de Actividades del PSC según la PC/DPC y legislación vigente.

5.7.4. Continuidad de negocio después de un desastre

352. La FNMT-RCM cuenta con un Plan de continuidad de negocio que describe las actuaciones a llevar a cabo en casos de desastre.

353. Se dispone de un 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. Mediante el uso de sistemas de copias de seguridad planificadas se protegen los datos necesarios para reanudar las operaciones de las Autoridades de Certificación.

354. 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.

355. 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

356. 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.

357. 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.

358. 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.

359. 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, y
- destruirá las Claves 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

360. 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.

361. Siguiendo dicho procedimiento, la FNMT-RCM preparará y seguirá un script de generación de claves. Un auditor cualificado será testigo del proceso de generación de pares de claves de CA y emitirá un informe en el que reflejará su opinión sobre el cumplimiento de la CA en la ejecución de la ceremonia de claves durante el proceso de generación de claves y certificados y los controles utilizados para garantizar la integridad y confidencialidad del par de claves.

362. 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.

363. 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*.

364. 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.

365. La generación de las *Claves* y la protección de la *Clave Privada*, se realizan garantizando las necesarias medidas de confidencialidad, usando sistemas de hardware y software seguros y de confianza conforme a las normas EESSI CWA14167-1 y CWA14167-2, además de tomar las precauciones necesarias para prevenir su pérdida, revelación, modificación o su uso sin autorización, de acuerdo con los requisitos de seguridad especificados en las normas EESSI aplicables a los *Prestadores de servicios de confianza*.

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

367. 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

368. No estipulado

6.1.1.3 Generación del par de Claves de los Suscriptores

369. Las *Claves privadas* de los *Certificados de autenticación de sitios web* son generadas y custodiadas por el *Suscriptor* del *Certificado*. La Autoridad de Certificación (AC) rechazará cualquier solicitud de certificado si se cumple alguna de las siguientes condiciones:

1. El par de claves no cumple con los requisitos establecidos en las Secciones 6.1.5 y/o 6.1.6 de los Requisitos Baseline (BR).
2. Existe evidencia clara de que el método específico utilizado para generar la Clave Privada es defectuoso.
3. La AC tiene conocimiento de un método demostrado o probado que pueda exponer la Clave Privada del solicitante a riesgo.
4. La AC ha sido notificada previamente de que la Clave Privada del solicitante sufrió una vulneración de clave, utilizando el procedimiento de revocación descrito en las Secciones 4.9.3 y 4.9.12.
5. La Clave Pública corresponde a una Clave Privada débil reconocida por la industria, incluyendo vulnerabilidades conocidas como Debian weak keys, ROCA y Close Primes, aplicando los métodos de verificación específicos de cada caso.

6.1.2. Envío de la clave privada al suscriptor

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

6.1.3. Envío de la clave pública al emisor del certificado

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

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

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

6.1.5. Tamaños de claves y algoritmos utilizados

373. Los algoritmos utilizados bajo el ámbito de la presente PC/DPC son:

- ECDSA-with-SHA384.
- RSA-with-SHA384.

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

- Claves de la AC FNMT raíz: ECC P-384 bits.
- Claves de la AC FNMT raíz G2R: 4096 bits.
- Claves de las AC Subordinadas: ECC P-384 bits.
- Claves de las AC Subordinadas G2R: 4096 bits.
- Claves de los *Certificados de autenticación de sitios web:* ECC P-384 bits o 3072 bits.

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

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

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

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

377. Los *Certificados* raíz de las AC tienen habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las AC Subordinadas y las ARLs. Los *Certificados* de las AC Subordinadas que expiden los *Certificados de autenticación de sitios web* tienen habilitado exclusivamente el uso para firmar/sellar *Certificados* de usuario final (*Certificados de autenticación de sitios web*) y CRLs. Adicionalmente, los tipos G2 de estos *Certificados* cuentan con el uso extendido de clave de autenticación de servidor (server authentication).

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

379. Los *Certificado de autenticación de sitios web* emitidos por AC Servidores Seguros Tipo1 y AC Servidores Seguros Tipo2 cuentan también con el uso extendido de autenticación de cliente (client authentication).

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

380. La FNMT-RCM protegerá sus claves privadas de acuerdo con las disposiciones de esta *PC/DPC* y en cumplimiento con CA/Browser Forum's Baseline Requirements.

6.2.1. Estándares para los módulos criptográficos

381. 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 de un dispositivo criptográfico certificado conforme a Common Criteria (ISO/IEC 15408), con nivel de aseguramiento EAL4+ incluyendo el componente ALC_FLR.2 and AVA_VAN.5. 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*.

382. 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*.

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

383. 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 simultáneo n de m (2 de 5).

6.2.3. Custodia de la clave privada

384. 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.

385. Las *Claves Privadas* de los *Titulares* son mantenidas, con un alto nivel de confianza, bajo el control exclusivo del propio *Titular*.

6.2.4. Copia de seguridad de la clave privada

386. Las copias de seguridad de las claves privadas de CA deben ser respaldadas por varias personas con rol de confianza y solo se almacenarán de forma cifrada en módulos criptográficos que cumplan con los requisitos especificados en la Sección 6.2.1.

6.2.5. Archivado de la clave privada

387. Sólo 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.

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

388. 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*". En caso de que se deba transferir una clave privada de un módulo criptográfico a otro, la clave privada se deberá cifrar durante la transferencia. Las claves privadas nunca existirán en forma de texto sin formato fuera del módulo criptográfico.

6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

389. 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.

390. 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.

391. Las claves privadas de la CA raíz de la FNMT-RCM se generan y almacenan dentro de módulos criptográficos que cumplen con los requisitos de 6.2.1 de esta *PC/DPC.*

6.2.8. Método de activación de la clave privada

392. Las *Claves Privadas* de las Autoridades de Certificación son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad conforme a Common Criteria (ISO/IEC 15408), con nivel de aseguramiento EAL4+ incluyendo el componente ALC_FLR.2 and AVA_VAN.5.

6.2.9. Método de desactivación de la clave privada

393. 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".

6.2.10. Método de destrucción de la clave privada

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

6.2.11. Clasificación de los módulos criptográficos

395. 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

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

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

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

- *Certificado* de las AC raíces y su par de *Claves*: véase el apartado "1.3.1. Autoridad de Certificación" de la presente PC/DPC.

- El *Certificado* de la AC subordinada que expide los *Certificados de autenticación de sitios web* y su par de *Claves*: véase el apartado "1.3.1. Autoridad de Certificación" de la presente PC/DPC.
- Los *Certificados de autenticación de sitios web* y su par de *Claves:* el periodo máximo de vigencia es de 199 días.

398. A efectos del cálculo de tiempos, se considera que un día equivale a 86400 segundos. Cualquier cantidad mayor que ésta, incluidas las fracciones de segundo y/o los segundos intercalares, dará lugar a un día adicional.

6.4. DATOS DE ACTIVACIÓN

6.4.1. Generación e instalación de datos de activación

399. 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*.

6.4.2. Protección de datos de activación

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

6.4.3. Otros aspectos de los datos de activación

401. No estipulados.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1. Requisitos técnicos específicos de seguridad informática

402. 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.

403. La FNMT-RCM requiere la autenticación multifactor para todas las cuentas capaces de generar directamente la emisión del certificado.

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

6.5.1.1 Comunicación de las incidencias de seguridad

405. 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

406. 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

407. 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

408. 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

409. 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.

410. 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.

411. 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

412. 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.

413. 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.

414. La FNMT-RCM comprueba una vez al mes si existen actualizaciones disponibles sobre las herramientas de linting de certificados de terceras partes que utiliza.

6.6.2. Controles de gestión de la seguridad

415. 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.

416. 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

417. 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 su política de backup y restauración.

6.6.3.1 Actualización de algoritmia

418. 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 RED

419. 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.

420. 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.

421. 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.

422. 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 con el fin de

- Comprobar que los controles de seguridad de la red cumplen con los requisitos de seguridad de la red y del sistema de certificación.
- Revisar la monitorización, contraseñas, etc. para detectar signos de intrusión o debilidad.
- Asegurarse de que el sistema de detección de intrusos y otro software de supervisión están actualizados.
- Confirmar la capacidad de interrumpir rápidamente la emisión de certificados si se alerta de una intrusión.

423. 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.

424. 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.

425. 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

426. 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.

7. PERFILES DE LOS CERTIFICADOS, CRLS Y OCSP

7.1. PERFIL DEL CERTIFICADO

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

428. Los *Certificados* expedidos con políticas EV (*Certificado de Sede electrónica*, *Certificado EV* y *Certificado SAN EV*) contienen el identificador de política 0.4.0.2042.1.4, 2.23.140.1.1 y 0.4.0.194112.1.4.

429. Los *Certificados* expedidos con políticas OV (*Certificado OV*, *Certificado Wildcard OV* y *Certificado SAN OV*) contienen el identificador de política 0.4.0.2042.1.7 y 2.23.140.1.2.2.

7.1.1. Número de versión

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

7.1.2. Extensiones del certificado

431. Las extensiones definidas para los certificados X.509 v3 de la FNMT-RCM proporcionan métodos para asociar atributos adicionales con usuarios o claves públicas y para administrar la jerarquía de certificación. Cada extensión del certificado es marcada como crítica o no crítica.

432. Las extensiones de certificado, su criticidad y los algoritmos criptográficos de los identificadores se proporcionan de acuerdo con los estándares IETF RFC 5280 y /o cumplen con los requisitos CAB Forum "Baseline Requirements" y "EV Guidelines" cuando corresponda.

433. Los documentos que describen el perfil de los *Certificados de autenticación de sitios web*, incluyendo todas sus extensiones son publicados en:

AC SERVIDORES SEGUROS TIPO 1:

https://www.sede.fnmt.gob.es/documents/10445900/10575386/Perfiles_certificados_servidores_seguros_tipo1.pdf

AC SERVIDORES SEGUROS TIPO 2:

https://www.sede.fnmt.gob.es/documents/10445900/10575386/Perfiles_certificados_servidores_seguros_tipo2.pdf

7.1.3. Identificadores de objeto de algoritmos

434. Los identificadores de objeto (OID) correspondiente a los algoritmos criptográficos utilizados son:

- Jerarquía RSA: Algoritmo SHA-384 with RSA cuyo OID es 1.2.840.113549.1.1.12.
- Jerarquías Curva Elíptica: Algoritmo SHA-384 with ECDSA cuyo OID es 1.2.840.10045.4.3.3

7.1.4. Formatos de nombres

435. A la fecha de emisión, toda la información del titular es precisa y se han verificado todos los atributos presentes en el campo *Subject* del certificado.

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

437. Los *Certificados de autenticación de sitios web* deben contener una extensión Subject Alternative Name (SAN) válida y completa. La entrada dNSName en la extensión SAN debe contener o bien un FQDN o un nombre de dominio Wildcard que la CA haya previamente validado conforme a la sección 3.2.2.4.

438. Los *Certificados de autenticación de sitios web* 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.

439. Los *Certificados de autenticación de sitios web* no deben contener el carácter ("_") en las entradas dNSName.

440. Los campos OU quedan restringidos a la información del *Subscriptor* que ha sido verificada conforme a la sección 3 de la presente *PC/DPC*.

441. Los nombres de dominio Wildcard deben ser validados de conformidad con lo establecido en la sección 3.2.2.6. no pudiendo contener un nombre interno.

442. El FQDN o la parte del FQDN de un *Certificado Wildcard* sólo puede contener etiquetas *P-Labels* o *Non-Reserved LDH Labels*.

443. El campo "OrganizationIdentifier" del Subject sigue la norma ETSI EN 319 412-1.

444. El campo "SerialNumber" contiene el NIF del *Suscriptor*.

7.1.5. Restricciones de nombres

445. Las CAs subordinadas que emiten los certificados bajo la presente *PC/DPC* no están restringidas técnicamente.

7.1.6. Identificador de objeto de política de certificado

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

7.1.7. Empleo de la extensión restricciones de política

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

7.1.8. Sintaxis y semántica de los calificadores de política

448. La extensión "Certificate Policies" incluye un campo de "Policy Qualifiers":

- CPSPointer: contiene la URL donde se publican las *Políticas de Certificación* y *Prácticas de Servicios de confianza* aplicables a este servicio.

7.1.9. Tratamiento semántico para la extensión "Certificate policy"

449. 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 el campo relacionado en el apartado anterior.

7.2. PERFIL DE LA CRL

7.2.1. Número de versión

450. Los perfiles de las CRLs son conformes con el estándar X.509 versión 2.

7.2.2. CRL y extensiones

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

Tabla 8 – Perfiles de las CRLs

Campos y extensiones	Valor
Versión	V2
Algoritmo de firma	ecdsa-with-Sha384 o rsa-with-Sha384
Número de CRL	INTEGER ≥ 0 y < 2^{159}, asignado de manera estrictamente creciente a cada CRL emitida por la Autoridad de Certificación.
Emisor	DN del emisor
Fecha de emisión	Tiempo UTC de emisión.

Campos y extensiones	Valor
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
Certificados revocados	Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación

7.3. PERFIL DE OCSP

452. 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

453. 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

454. 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.

455. 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

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

457. Así mismo, para los *Certificados* que tienen la consideración de cualificados, son sometidos a la auditoría 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".

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

459. 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).

460. 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

461. Las auditorías ETSI mencionadas en el apartado anterior se realizan anualmente.

462. En el caso de los *Certificados* con la consideración de cualificados (*Certificado de Sede electrónica*, *Certificado EV* y *Certificado SAN EV*) la auditoría garantiza adicionalmente el cumplimiento de los requisitos de los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-4 "Certificate profile for web site certificates".

463. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente y con CAB Forum's Baseline Requirements y EV Guidelines. El período operativo durante el cual la Autoridad de Certificación emite certificados deberá estructurarse en una secuencia continua e ininterrumpida de periodos de auditoría. Cada periodo de auditoría no podrá exceder una duración máxima de un (1) año.

8.2. CUALIFICACIÓN DEL AUDITOR

464. El auditor que verifique y compruebe la correcta operativa del *Prestador de Servicios de Confianza* de la FNMT-RCM deberá ser un auditor cualificado, es decir, 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.

465. 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

466. 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.

467. 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.

468. 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

469. 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

470. 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.

471. 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.

472. 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

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

474. La FNMT-RCM hará público el informe de auditoría a más tardar tres meses después de finalizado el período de auditoría.

8.7. AUTOEVALUACIÓN

475. 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.

476. La FNMT realiza un proceso de linting para verificar la exactitud técnica de los certificados dentro del conjunto de muestras seleccionado, de manera independiente a cualquier linting previo realizado sobre esos mismos certificados.

9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

477. 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.

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

9.1.1. Tarifas de emisión o renovación de certificados

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

9.1.2. Tarifas de acceso a los certificados

480. No estipulado.

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

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

9.1.4. Tarifas para otros servicios

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

9.1.5. Política de reembolso

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

9.2. RESPONSABILIDAD FINANCIERA

484. 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, 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

485. La 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

486. No estipuladas.

9.2.3. Seguros y garantías para entidades finales

487. No estipuladas.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

9.3.1. Alcance de la información confidencial

488. 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

489. 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*.

490. Cualquier información cuya publicidad sea impuesta normativamente.

9.3.3. Responsabilidad para proteger la información confidencial

491. 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 DE CARÁCTER PERSONAL

492. 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

493. 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

494. 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*.

495. 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.

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

9.4.3. Información no considerada privada

497. 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

498. 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.

499. 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

500. 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

501. 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:

- Finalidad

- Entidad responsable
- Categorías de datos personales
- Quién proporciona los datos
- Quién es el afectado de los datos personales
- Quiénes son los encargados del tratamiento
- Comunicaciones de datos
- Transferencias internacionales de datos
- Plazo de supresión
- Medidas de seguridad

502. 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

503. 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

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

9.4.4.5 Notificación de violaciones de seguridad

505. La FNMT-RCM notificará a la Agencia Española de Protección de Datos (AEPD) cualquier violación de seguridad[4] 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.

506. 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.

[4] 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.

9.4.5. Aviso y consentimiento para usar información privada

507. 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

508. 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

509. No estipuladas.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

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

512. La FNMT-RCM mantiene todo derecho, título y participación sobre todos los derechos de propiedad intelectual e industrial y conocimientos relativos a la presente *PC/DPC*, los servicios que preste, y los programas de ordenador o hardware que utilice en dicha prestación de servicios. Cualquier otro uso distinto de la visualización, incluyendo la reproducción, redistribución y/o modificación de la presente declaración, queda prohibido sin la expresa autorización de la FNMT-RCM.

513. 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

514. 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*.

515. 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.

516. 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

9.6.1. Obligaciones de la AC

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

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

519. La FNMT-RCM emite los *Certificados de autenticación de sitios web* de conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser Forum y que pueden consultarse en la dirección https://cabforum.org/baseline-requirements-documents/ Asimismo, adaptará sus prácticas de expedición de dichos *Certificados* a la versión vigente de los citados requisitos. En caso de cualquier incoherencia entre la presente *PC/DPC* y la citada versión, dichos requisitos prevalecerán sobre este documento.

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

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

522. Con carácter previo a la expedición del *Certificado*

- Implementar un procedimiento que verifique que el Suscriptor posee el control o derecho de uso del nombre o nombres de dominio que aparecen en la extensión subjectAltName.
- Verificar que el *Solicitante* del Certificado ha reconocido y aceptado los Términos y Condiciones de uso.
- Comprobar la identidad y circunstancias personales del *Solicitante* del *Certificado* y del *Suscriptor* y/o su *Representante* y recoger la manifestación de que el *Solicitante* está autorizado por el *Suscriptor* para realizar la solicitud.

  La identificación se realizará a través de *Certificados* cualificados de firma electrónica admitidos en los procesos de FNMT-RCM.
- En el proceso de registro, comprobar los datos relativos a la personalidad jurídica del *Suscriptor* y a la capacidad del *Representante*. Todas estas comprobaciones se realizarán según lo dispuesto en las *Prácticas de Certificación Particulares* expresadas en este documento y según los protocolos y procedimientos de registro de la FNMT-RCM.

  En los procesos de comprobación de los extremos antes señalados anteriormente la FNMT-RCM podrá realizar verificaciones mediante la intervención de terceros que ostenten facultades fedatarias o de registros públicos o privados.
- Verificar que toda la información contenida en la solicitud del *Certificado* se corresponde con la aportada por el *Solicitante*.
- Comprobar que el *Solicitante* está en posesión de la *Clave Privada* asociada a la *Clave Pública* que se incorpora al *Certificado* a emitir.
- Garantizar que los procedimientos seguidos aseguran que las *Claves Privadas* correspondientes a los *Certificados de autenticación de sitios web* son generadas sin que se realicen copias ni se produzca el almacenamiento de los mismos por parte de la FNMT-RCM.
- Realizar la comunicación de información al *Suscriptor, Representante* y *Solicitante* de tal forma que se procure su *Confidencialidad*.
- Poner a disposición del *Solicitante, Suscriptor, Representante* y demás interesados (http://www.ceres.fnmt.es) la *Declaración de Prácticas de Certificación* y cuanta información sea relevante para el desarrollo de los procedimientos relacionados con el ciclo de vida de los *Certificados* objeto de esta *Política de Certificación* y *Prácticas de Certificación Particulares* de conformidad con la normativa aplicable.
- Garantizar que se mantiene un repositorio público accesible 24x7 para consultar la información actual del estado de los certificados (válido o revocado) de todos los certificados activos.
- Proceder a la revocación de los certificados que cumplan cualquiera de las razones de revocación que se especifican en este documento y en las guías de requerimientos de CA/Browser Forum.

9.6.2. Obligaciones de la AR

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

524. La AR, a través del Área de Registro de la FNMT-RCM, tiene las siguientes obligaciones:

- Con carácter general, seguir los procedimientos establecidos por la FNMT-RCM en la *Política y Prácticas de Certificación* de aplicación en el desempeño de sus funciones de gestión, expedición y revocación de *Certificados* y no alterar dicho marco de actuación.
- En particular, comprobar la identidad, y cualesquiera circunstancias personales relevantes para la finalidad asignada, de los *Solicitantes* de los *Certificados*, *Suscriptores* y sus *Representantes*, utilizando cualquiera de los medios admitidos en Derecho y conforme a lo previsto con carácter general en *PC/DPC.*
- Comprobar que la titularidad del nombre de dominio se corresponde con la identidad del *Suscriptor* o, en su caso, obtener la autorización de éste, que se asociará al *Certificado de autenticación de sitios web*, por los medios a su alcance que, razonablemente, permitan acreditar tal titularidad, de conformidad con el estado de la técnica.
- Recoger expresamente la manifestación del *Suscriptor* en relación con la titularidad del dominio del *Certificado de autenticación de sitios web*, manifestando que tiene el poder único de decisión sobre el mismo.
- Conservar toda la información y documentación relativa a los *Certificados*, cuya solicitud, renovación o revocación gestiona durante quince (15) años.
- Realizar la recepción y gestión de las solicitudes y los contratos de expedición (formulario pdf) de *Certificados* con el *Suscriptor* de los mismos.
- Comprobar diligentemente las causas de revocación que pudieran afectar a la vigencia de los *Certificados*.

9.6.3. Obligaciones de los Suscriptores

525. La FNMT-RCM exigirá, como parte de los términos y condiciones de uso, que el Solicitante asuma los compromisos y garantías establecidos en esta sección. El certificado no se emitirá hasta que el Solicitante acepte los términos y condiciones de uso.

526. 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.

527. 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.

528. El *Suscriptor* 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*.

529. 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 *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.

530. Esta información se recoge con la finalidad de prestar los servicios de confianza de los que son usuarios dichos *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 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.

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

532. Los *Suscriptores* han de tener el control del nombre de dominio de sitio web incluido en dichos *Certificados* y mantener bajo su uso exclusivo las *Claves privadas* asociadas.

533. El *Solicitante* y el *Suscriptor* de los *Certificados* expedidos bajo la presente *PC/DPC*, tienen la obligación de:

- No usar el *Certificado* fuera de los límites especificados en la presente *Política y Prácticas de Certificación* particulares.
- No usar el *Certificado* en caso de que el *Prestador de Servicios de Confianza* haya cesado su actividad como Entidad emisora de *Certificados* que expidió el certificado en cuestión, especialmente en los casos en los que los *Datos de Creación de Sello* del prestador puedan estar comprometidos, y así se haya comunicado.
- Aportar información veraz en la solicitud de los *Certificados* y mantenerla actualizada, suscribiendo los contratos por persona con capacidad suficiente.
- No solicitar para el *Sujeto* del certificado signos distintivos, denominaciones o derechos de propiedad industrial o intelectual de las que no sea titular, licenciatario o cuente con autorización demostrable para su uso.
- Instalar el certificado únicamente en servidores accesibles en los nombres alternativos del sujeto (subjectAltName) que figuran en el certificado, y de utilizar el certificado únicamente de conformidad con todas las leyes aplicables y con el acuerdo de suscripción o las condiciones de uso.
- Actuar con diligencia respecto de la custodia y conservación de los *Datos de creación de Firma / Sello* o cualquier otra información sensible como *Claves*, códigos de activación del *Certificado*, palabras de acceso, números de identificación personal, etc., así como de los soportes de los *Certificados,* lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.

- Conocer y cumplir las condiciones de utilización de los *Certificados* previstas en las condiciones de uso y en la *Declaración de Prácticas de Certificación* y en particular, las limitaciones de uso de los *Certificados*
- Conocer y cumplir las modificaciones que se produzcan en la *Declaración de Prácticas de Certificación*.
- Solicitar la revocación del correspondiente *Certificado*, según el procedimiento descrito en el presente documento, notificando diligentemente a la FNMT-RCM las circunstancias para la revocación o sospecha de pérdida de la *Confidencialidad*, la divulgación, modificación o uso no autorizado de las *Claves privadas* asociadas,
- Revisar la información contenida en el *Certificado*, y notificar a la FNMT-RCM cualquier error o inexactitud.
- Verificar con carácter previo a confiar en los *Certificados,* la *Firma electrónica* o el *Sello electrónico* avanzados del *Prestador de Servicios de Confianza* emisor del *Certificado.*
- Notificar diligentemente a la FNMT-RCM cualquier modificación de los datos aportados en la solicitud del *Certificado*, solicitando, cuando consecuentemente fuere pertinente, la revocación del mismo.

534. Será en todo caso responsabilidad del Suscriptor utilizar de manera adecuada y custodiar diligentemente el *Certificado*, según el propósito y función para el que ha sido expedido, así como informar a la FNMT-RCM acerca de cualquier variación de estado o información respecto de lo reflejado en el Certificado, para su revocación y nueva expedición.

535. Asimismo, será el *Suscriptor* quien deba responder, en todo caso, ante la FNMT-RCM, las Entidades usuarias y, en su caso, ante terceros, del uso indebido del *Certificado*, o de la falsedad o errores de las manifestaciones en él recogidas, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

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

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

- No realizar registros o tramitar solicitudes de *Certificados de Sede electrónica* por personal que preste sus servicios en una entidad diferente a la que representa como Oficina de Registro, salvo habilitación expresa de otra entidad.
- No realizar registros o tramitar solicitudes de *Certificados* emitidos bajo esta política y cuyo *Suscriptor* se corresponda con una entidad pública sobre la que no tenga potestades o no tenga competencias para actuar como *Oficina de Registro*.

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

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

9.6.4. Obligaciones de las partes que confían

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

540. 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

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

542. Asimismo, será responsabilidad de la Entidad Usuaria observar lo dispuesto en la Declaración de Prácticas de Certificación y sus posibles modificaciones futuras, con especial atención a los límites de uso establecidos para los *Certificados* en esta Política de Certificación.

9.6.5. Obligaciones de otros participantes

543. No estipulado.

9.7. RENUNCIA DE GARANTÍAS

544. No estipulado.

9.8. LÍMITES DE RESPONSABILIDAD

545. 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*.

546. 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*.

547. La 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.

548. 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.

549. 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.

550. 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 de Prácticas de Certificación* y en la Ley.

551. 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.

552. 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.

553. 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.

554. 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.

555. 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

556. 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

557. No estipulado.

9.9.2. Indemnización de los Suscriptores

558. No estipulado.

9.9.3. Indemnización de las partes que confían

559. No estipulado.

9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. Plazo

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

9.10.2. Terminación

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

9.10.3. Efectos de la finalización

562. Para los certificados vigentes emitidos bajo una *Declaración de Políticas y Prácticas 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

563. 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*.

564. 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.

565. 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

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

9.12.2. Periodo y mecanismo de notificación

567. 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.

568. 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

569. 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

570. 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

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

572. 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 modificado por el modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital.

573. 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.
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TSL Server Certificates
- CA/Browser Forum EV Guidelines
- Norma de accesibilidad web UNE-EN 301 549
- Chrome Root Program Policy, Mozilla Root Store Policy, Microsoft Trusted Root Program and Apple Root Certificate Program
- CCADB Policy

574. 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).

575. 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.

576. 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

577. La FNMT-RCM manifiesta su compromiso de cumplimiento de la normativa y de los requisitos de aplicación a cada tipo de *Certificado de autenticación de sitios web*, recogidos

en el apartado 9.1.4, incluyendo las consideraciones establecidas en el apartado "1.5.4. Procedimiento de aprobación de la DPC" del presente documento de *PC/DPC*.

9.16. ESTIPULACIONES DIVERSAS

9.16.1. Acuerdo íntegro

578. Los *Titulares* y terceros que confían en los Certificados asumen en su totalidad el contenido de la presente *Declaración de Políticas y Prácticas de Certificación.*

9.16.2. Asignación

579. 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

580. En caso de conflicto de cualquier parte de este documento con la legislación vigente de cualquier jurisdicción en la que una Autoridad de Certificación opere o emita certificados, tras la correspondiente revisión legal, la FNMT-RCM podrá modificar los puntos conflictivos en la medida mínima necesaria para cumplir con dicha legislación.

581. En tal caso, (antes de emitir un certificado bajo los requisitos modificados) FNMT-RCM incluirá en los subapartados de esta sección información sobre la Ley que requiere la modificación y el cambio específico implementado por FNMT-RCM.

582. La FNMT-RCM también informará a las partes interesadas, como el CAB Forum, de la información relevante recién añadida antes de emitir un certificado bajo los cambios realizados

583. Las modificaciones que la FNMT-RCM realice en sus prácticas bajo este apartado cesarán en el momento en que la Ley ya no esté vigente, o si los requisitos cambian de tal manera que permita a la CA cumplir con la Ley y con los requisitos del CABForum al mismo tiempo. En ese caso, en un plazo de 90 días, la FNMT-RCM debe ajustar sus prácticas, actualizar su Declaración de Prácticas de Certificación y notificar al CA/Browser Forum.

9.16.4. Cumplimiento

584. No estipulado.

9.16.5. Fuerza Mayor

585. No estipulado.

9.17. OTRAS ESTIPULACIONES

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

587. 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.

588. 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/).

589. 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.

590. 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 y paralizando la expedición de certificados sobre dichos dispositivos.

591. 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 "CERES-Organización del Departamento" 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.

592. 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.

593. 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".

ANEXO I: PERFIL DEL CERTIFICADO AC RAIZ FNMT-RCM SERVIDORES SEGUROS

Campo		Contenido	Ext. Critica
1. Version		2	
2. Serial Number		Número identificativo único del certificado.	
3. Signature Algorithm		ecdsa-with-SHA384	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	
	4.1. Country	C=ES	
	4.2 Organization	O=FNMT-RCM	
	4.3 Organization Unit	OU=Ceres	
	4.4 OrganizationIddentifier	VATES- Q2826004J	
	4.5 CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
5. Validity		25 años	
6. Subject			
	6.1. Country	C=ES	
	6.2. Organization	O=FNMT-RCM	
	6.3. Organization Unit	OU=Ceres	
	6.4. OrganizationIddentifier	VATES- Q2826004J	
	6.5. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
7. Subject Public Key Info		ECC P-384 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	
	9.5. Key Agreement	0	
	9.6. Key Certificate Signature	1	
	9.7. CRL Signature	1	
10. Basic Constraints			Sí
	10.1. cA	Valor TRUE (CA)	
	10.2. pathLenConstraint	Ninguna	

ANEXO II: PERFIL DEL CERTIFICADO AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R

Campo		Contenido	Ext. Critica
1. Version		2	
2. Serial Number		Número identificativo único del certificado.	
3. Signature Algorithm		Sha384WithRSAEncryption	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	
	4.1. Country	C=ES	
	4.6 Organization	O=FNMT-RCM	
	4.7 CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R	
5. Validity		15 años	
6. Subject			
	6.1. Country	C=ES	
	6.2. Organization	O=FNMT-RCM	
	6.3. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS G2R	
7. Subject Public Key Info		RSA 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	
	9.5. Key Agreement	0	
	9.6. Key Certificate Signature	1	
	9.7. CRL Signature	1	
10. Basic Constraints			Sí
	10.1. cA	Valor TRUE (CA)	
	10.2. pathLenConstraint	Ninguna	