



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

## **POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN PARTICULARES DE CERTIFICADOS DE CARRERA JUDICIAL**

|                | <b>NOMBRE</b> | <b>FECHA</b> |
|----------------|---------------|--------------|
| Elaborado por: | FNMT-RCM      | 11/09/2024   |
| Revisado por:  | FNMT-RCM      | 11/09/2024   |
| Aprobado por:  | FNMT-RCM      | 11/09/2024   |

| <b>Versión</b> | <b>Fecha</b> | <b>Descripción</b>   |
|----------------|--------------|--|
| 1.0            | 11/09/2024   | Creación del documento: Declaración de Políticas y Prácticas de Certificación particulares de certificados de Carrera Judicial |
|                |              |  |
|                |              |  |
|                |              |  |
|                |              |  |
|                |              |  |
|                |              |  |

**Referencia:** DPC/DPCCJ\_0100/SGPSC/2024

**Documento clasificado como:** *Público*

## Índice de contenidos

|  |           |
|--|-----------|
| <b>1. Introducción.....</b>  | <b>9</b>  |
| 1.1. Objeto.....   | 9         |
| 1.2. Nombre del documento e identificación.....  | 10        |
| 1.3. Partes intervinientes.....  | 12        |
| 1.3.1. Autoridad de Certificación.....   | 12        |
| 1.3.2. Autoridad de Registro.....  | 14        |
| 1.3.3. Firmantes.....  | 14        |
| 1.3.4. Suscriptores de los certificados.....   | 14        |
| 1.3.5. Partes que confían.....   | 14        |
| 1.3.6. Otros participantes.....  | 15        |
| 1.4. Uso de los certificados.....  | 15        |
| 1.4.1. Usos permitidos de los certificados.....  | 15        |
| 1.4.2. Restricciones en el uso de los certificados.....  | 15        |
| 1.5. Administración de Políticas.....  | 17        |
| 1.5.1. Entidad responsable.....  | 17        |
| 1.5.2. Datos de contacto.....  | 17        |
| 1.5.3. Responsables de adecuación de la DPC.....   | 17        |
| 1.5.4. Procedimiento de aprobación de la DPC.....  | 17        |
| 1.6. Definiciones y Acrónimos.....   | 18        |
| 1.6.1. Definiciones.....   | 18        |
| 1.6.2. Acrónimos.....  | 19        |
| <b>2. Publicación y repositorios.....</b>  | <b>20</b> |
| 2.1. Repositorio.....  | 20        |
| 2.2. Publicación de información de certificación.....  | 20        |
| 2.3. Frecuencia de publicación.....  | 20        |
| 2.4. Control de acceso a los repositorios.....   | 20        |
| <b>3. Identificación y autenticación.....</b>  | <b>20</b> |
| 3.1. Nombres.....  | 20        |
| 3.1.1. Tipos de nombres.....   | 21        |
| 3.1.2. Significado de los nombres.....   | 21        |
| 3.1.3. Seudónimos.....   | 21        |
| 3.1.4. Reglas utilizadas para interpretar varios formatos de nombres.....  | 21        |
| 3.1.5. Unicidad de los nombres.....  | 21        |
| 3.1.6. Reconocimiento y autenticación de marcas registradas.....   | 21        |
| 3.2. Validación inicial de la identidad.....   | 22        |
| 3.2.1. Métodos para probar la posesión de la clave privada.....  | 22        |
| 3.2.2. Autenticación de la identidad de la organización.....   | 22        |
| 3.2.3. Autenticación de la identidad de la persona física solicitante.....   | 22        |
| 3.2.3.1. Comprobación directa mediante presencia física.....   | 23        |
| 3.2.3.2. Comprobación indirecta mediante medios de aseguramiento equivalente a la presencia física de conformidad con el Derecho nacional..... | 23        |



|           |  |           |
|-----------|--|-----------|
| 3.2.4.    | Información no verificada del Suscriptor.....  | 23        |
| 3.2.5.    | Validación de la autorización.....   | 23        |
| 3.2.6.    | Criterios de interoperación.....   | 24        |
| 3.3.      | <i>Identificación y autenticación para peticiones de renovación de claves</i> .....    | 24        |
| 3.3.1.    | Renovación rutinaria.....  | 24        |
| 3.3.2.    | Renovación después de una revocación.....  | 24        |
| 3.4.      | <i>Identificación y autenticación para peticiones de revocación</i> .....              | 24        |
| <b>4.</b> | <b>Requisitos operativos del ciclo de vida de los certificados</b> .....               | <b>24</b> |
| 4.1.      | <i>Solicitud de Certificados</i> .....   | 24        |
| 4.1.1.    | Quién puede solicitar un Certificado.....  | 24        |
| 4.1.2.    | Proceso de registro y responsabilidades.....   | 24        |
| 4.2.      | <i>Procedimiento de solicitud de certificados</i> .....                                | 25        |
| 4.2.1.    | Realización de las funciones de identificación y autenticación.....                    | 25        |
| 4.2.2.    | Aprobación o rechazo de la solicitud del certificado.....                              | 25        |
| 4.2.3.    | Tiempo en procesar la solicitud.....   | 26        |
| 4.3.      | <i>Emisión del certificado</i> .....   | 26        |
| 4.3.1.    | Acciones de la AC durante la emisión.....  | 26        |
| 4.3.2.    | Notificación de la emisión.....  | 27        |
| 4.4.      | <i>Aceptación del certificado</i> .....  | 27        |
| 4.4.1.    | Proceso de aceptación.....   | 27        |
| 4.4.2.    | Publicación del certificado por la AC.....   | 27        |
| 4.4.3.    | Notificación de la emisión a otras entidades.....                                      | 28        |
| 4.5.      | <i>Par de claves y uso del certificado</i> .....                                       | 28        |
| 4.5.1.    | Clave privada y uso del certificado.....   | 28        |
| 4.5.2.    | Uso del certificado y la clave pública por terceros que confían.....                   | 28        |
| 4.6.      | <i>Renovación del certificado</i> .....  | 28        |
| 4.6.1.    | Circunstancias para la renovación del certificado.....                                 | 28        |
| 4.6.2.    | Quién puede solicitar la renovación del certificado.....                               | 28        |
| 4.6.3.    | Procesamiento de solicitudes de renovación del certificado.....                        | 28        |
| 4.6.4.    | Notificación de la renovación del certificado.....                                     | 28        |
| 4.6.5.    | Conducta que constituye la aceptación de la renovación del certificado.....            | 29        |
| 4.6.6.    | Publicación del certificado renovado.....  | 29        |
| 4.6.7.    | Notificación de la renovación del certificado a otras entidades.....                   | 29        |
| 4.7.      | <i>Renovación con regeneración de las claves del certificado</i> .....                 | 29        |
| 4.7.1.    | Circunstancias para la renovación con regeneración de claves.....                      | 29        |
| 4.7.2.    | Quién puede solicitar la renovación con regeneración de claves.....                    | 29        |
| 4.7.3.    | Procesamiento de solicitudes de renovación con regeneración de claves.....             | 29        |
| 4.7.4.    | Notificación de la renovación con regeneración de claves.....                          | 29        |
| 4.7.5.    | Conducta que constituye la aceptación de la renovación con regeneración de claves..... | 29        |
| 4.7.6.    | Publicación del certificado renovado.....  | 29        |
| 4.7.7.    | Notificación de la renovación con regeneración de claves a otras entidades.....        | 30        |
| 4.8.      | <i>Modificación del certificado</i> .....  | 30        |
| 4.8.1.    | Circunstancias para la modificación del certificado.....                               | 30        |
| 4.8.2.    | Quién puede solicitar la modificación del certificado.....                             | 30        |
| 4.8.3.    | Procesamiento de solicitudes de modificación del certificado.....                      | 30        |
| 4.8.4.    | Notificación de la modificación del certificado.....                                   | 30        |



|           |   |           |
|-----------|---|-----------|
| 4.8.5.    | Conducta que constituye la aceptación de la modificación del certificado.....         | 30        |
| 4.8.6.    | Publicación del certificado modificado.....   | 30        |
| 4.8.7.    | Notificación de la modificación del certificado a otras entidades.....                | 30        |
| 4.9.      | <i>Revocación y Suspensión del certificado</i> .....                                  | 30        |
| 4.9.1.    | Circunstancias para la revocación.....  | 31        |
| 4.9.1.1   | Circunstancias para la revocación del certificado del suscriptor.....                 | 31        |
| 4.9.1.2   | Circunstancias para la revocación del certificado de la CA subordinada.....           | 32        |
| 4.9.2.    | Quién puede solicitar la revocación.....  | 33        |
| 4.9.3.    | Procedimiento de solicitud de la revocación.....                                      | 33        |
| 4.9.4.    | Periodo de gracia de la solicitud de revocación.....                                  | 34        |
| 4.9.5.    | Plazo de tiempo para procesar la solicitud de revocación.....                         | 34        |
| 4.9.6.    | Obligación de verificar las revocaciones por las partes que confían.....              | 34        |
| 4.9.7.    | Frecuencia de generación de CRLs.....   | 34        |
| 4.9.8.    | Periodo máximo de latencia de las CRLs.....   | 34        |
| 4.9.9.    | Disponibilidad del sistema de verificación online del estado de los certificados..... | 34        |
| 4.9.10.   | Requisitos de comprobación en línea de la revocación.....                             | 35        |
| 4.9.11.   | Otras formas de aviso de revocación disponibles.....                                  | 35        |
| 4.9.12.   | Requisitos especiales de revocación de claves comprometidas.....                      | 35        |
| 4.9.13.   | Circunstancias para la suspensión.....  | 35        |
| 4.9.14.   | Quién puede solicitar la suspensión.....  | 35        |
| 4.9.15.   | Procedimiento para la petición de la suspensión.....                                  | 35        |
| 4.9.16.   | Límites sobre el periodo de suspensión.....   | 35        |
| 4.10.     | <i>Servicios de información del estado de los certificados</i> .....                  | 35        |
| 4.10.1.   | Características operativas.....   | 35        |
| 4.10.2.   | Disponibilidad del servicio.....  | 35        |
| 4.10.3.   | Características opcionales.....   | 36        |
| 4.11.     | <i>Finalización de la suscripción</i> .....   | 36        |
| 4.12.     | <i>Custodia y recuperación de claves</i> .....  | 36        |
| 4.12.1.   | Prácticas y políticas de custodia y recuperación de claves.....                       | 36        |
| 4.12.2.   | Prácticas y políticas de protección y recuperación de la clave de sesión.....         | 36        |
| <b>5.</b> | <b>Controles de seguridad física, de procedimientos y de personal.....</b>            | <b>36</b> |
| 5.1.      | <i>Controles de Seguridad Física</i> .....  | 36        |
| 5.1.1.    | Ubicación de las instalaciones.....   | 36        |
| 5.1.2.    | Acceso Físico.....  | 36        |
| 5.1.3.    | Electricidad y Aire Acondicionado.....  | 36        |
| 5.1.4.    | Exposición al agua.....   | 37        |
| 5.1.5.    | Prevención y Protección contra incendios.....   | 37        |
| 5.1.6.    | Almacenamiento de Soportes.....   | 37        |
| 5.1.7.    | Eliminación de Residuos.....  | 37        |
| 5.1.8.    | Copias de Seguridad fuera de las instalaciones.....                                   | 37        |
| 5.2.      | <i>Controles de Procedimiento</i> .....   | 37        |
| 5.2.1.    | Roles de Confianza.....   | 37        |
| 5.2.2.    | Número de personas por tarea.....   | 37        |
| 5.2.3.    | Identificación y autenticación para cada rol.....                                     | 37        |
| 5.2.4.    | Roles que requieren segregación de funciones.....                                     | 37        |
| 5.3.      | <i>Controles de Personal</i> .....  | 37        |
| 5.3.1.    | Conocimientos, cualificación, experiencia y requerimientos acreditativos.....         | 37        |



|           |   |           |
|-----------|---|-----------|
| 5.3.2.    | Procedimientos de verificación de antecedentes .....                                  | 38        |
| 5.3.3.    | Requisitos de formación .....   | 38        |
| 5.3.4.    | Requisitos y frecuencia de actuación formativa.....                                   | 38        |
| 5.3.5.    | Secuencia y frecuencia de rotación laboral.....                                       | 38        |
| 5.3.6.    | Sanciones por acciones no autorizadas .....   | 38        |
| 5.3.7.    | Requisitos de contratación de personal.....   | 38        |
| 5.3.8.    | Suministro de documentación al personal.....  | 38        |
| 5.4.      | <i>Procedimientos de auditoría</i> .....  | 38        |
| 5.4.1.    | Tipos de eventos registrados .....  | 38        |
| 5.4.2.    | Frecuencia de procesamiento de registros .....  | 38        |
| 5.4.3.    | Periodo de conservación de los registros .....  | 38        |
| 5.4.4.    | Protección de los registros .....   | 38        |
| 5.4.5.    | Procedimientos de copias de seguridad de los registros auditados .....                | 39        |
| 5.4.6.    | Sistemas de recolección de registros.....   | 39        |
| 5.4.7.    | Notificación al sujeto causante de los eventos .....                                  | 39        |
| 5.4.8.    | Análisis de vulnerabilidades .....  | 39        |
| 5.5.      | <i>Archivado de registros</i> .....   | 39        |
| 5.5.1.    | Tipos de registros archivados.....  | 39        |
| 5.5.2.    | Periodo de retención del archivo.....   | 39        |
| 5.5.3.    | Protección del archivo .....  | 39        |
| 5.5.4.    | Procedimientos de copia de respaldo del archivo .....                                 | 39        |
| 5.5.5.    | Requisitos para el sellado de tiempo de los registros of Records .....                | 39        |
| 5.5.6.    | Sistema de archivo .....  | 39        |
| 5.5.7.    | Procedimientos para obtener y verificar la información archivada.....                 | 39        |
| 5.6.      | <i>Cambio de claves de la AC</i> .....  | 40        |
| 5.7.      | <i>Gestión de incidentes y vulnerabilidades</i> .....                                 | 40        |
| 5.7.1.    | Gestión de incidentes y vulnerabilidades.....   | 40        |
| 5.7.2.    | Actuación ante datos y software corruptos .....                                       | 40        |
| 5.7.3.    | Procedimiento ante compromiso de la clave privada de la AC.....                       | 40        |
| 5.7.4.    | Continuidad de negocio después de un desastre .....                                   | 40        |
| 5.8.      | <i>Cese de la actividad del Prestador de Servicios de Confianza</i> .....             | 40        |
| <b>6.</b> | <b>Controles de seguridad técnica.....</b>  | <b>40</b> |
| 6.1.      | <i>Generación e instalación de las Claves</i> .....                                   | 40        |
| 6.1.1.    | Generación del par de claves .....  | 40        |
| 6.1.1.1   | Generación del par de Claves de la CA.....  | 40        |
| 6.1.1.2   | Generación del par de Claves de la RA.....  | 40        |
| 6.1.1.3   | Generación del par de Claves de los Suscriptores.....                                 | 41        |
| 6.1.2.    | Envío de la clave privada al suscriptor .....   | 41        |
| 6.1.3.    | Envío de la clave pública al emisor del certificado.....                              | 41        |
| 6.1.4.    | Distribución de la clave pública de la AC a las partes que confían .....              | 41        |
| 6.1.5.    | Tamaños de claves y algoritmos utilizados.....  | 41        |
| 6.1.6.    | Parámetros de generación de la clave pública y verificación de la calidad.....        | 41        |
| 6.1.7.    | Usos admitidos de las claves (KeyUsage field X.509v3) .....                           | 42        |
| 6.2.      | <i>Protección de la clave privada y controles de los módulos criptográficos</i> ..... | 42        |
| 6.2.1.    | Estándares para los módulos criptográficos .....                                      | 42        |
| 6.2.2.    | Control multi-persona (n de m) de la clave privada.....                               | 42        |
| 6.2.3.    | Custodia de la clave privada .....  | 42        |



|           |  |           |
|-----------|--|-----------|
| 6.2.4.    | Copia de seguridad de la clave privada.....                                    | 42        |
| 6.2.5.    | Archivado de la clave privada.....   | 42        |
| 6.2.6.    | Trasferencia de la clave privada a o desde el módulo criptográfico .....       | 43        |
| 6.2.7.    | Almacenamiento de la clave privada en el módulo criptográfico .....            | 43        |
| 6.2.8.    | Método de activación de la clave privada .....                                 | 43        |
| 6.2.9.    | Método de desactivación de la clave privada.....                               | 43        |
| 6.2.10.   | Método de destrucción de la clave privada .....                                | 43        |
| 6.2.11.   | Clasificación de los módulos criptográficos .....                              | 43        |
| 6.3.      | <i>Otros aspectos de la gestión del par de claves .....</i>                    | <i>43</i> |
| 6.3.1.    | Archivo de la clave pública.....   | 43        |
| 6.3.2.    | Periodos de operación del certificado y periodos de uso del par de claves..... | 44        |
| 6.4.      | <i>Datos de activación .....</i>   | <i>44</i> |
| 6.4.1.    | Generación e instalación de datos de activación.....                           | 44        |
| 6.4.2.    | Protección de datos de activación .....  | 44        |
| 6.4.3.    | Otros aspectos de los datos de activación .....                                | 44        |
| 6.5.      | <i>Controles de seguridad informática .....</i>                                | <i>44</i> |
| 6.5.1.    | Requisitos técnicos específicos de seguridad informática .....                 | 44        |
| 6.5.2.    | Evaluación del nivel de seguridad informática .....                            | 45        |
| 6.6.      | <i>Controles técnicos del ciclo de vida .....</i>                              | <i>45</i> |
| 6.6.1.    | Controles de desarrollo de sistemas .....                                      | 45        |
| 6.6.2.    | Controles de gestión de la seguridad.....                                      | 45        |
| 6.6.3.    | Controles de seguridad del ciclo de vida .....                                 | 45        |
| 6.7.      | <i>Controles de seguridad de red.....</i>                                      | <i>45</i> |
| 6.8.      | <i>Fuente de tiempo .....</i>  | <i>45</i> |
| 6.9.      | <i>Otros controles adicionales.....</i>  | <i>45</i> |
| 6.9.1.    | Control de la capacidad de prestación de los servicios .....                   | 45        |
| 6.9.2.    | Control de desarrollo de sistemas y aplicaciones informáticas .....            | 45        |
| <b>7.</b> | <b>Perfiles de los certificados, CRLs y OCSP .....</b>                         | <b>45</b> |
| 7.1.      | <i>Perfil del certificado .....</i>  | <i>45</i> |
| 7.1.1.    | Número de versión.....   | 46        |
| 7.1.2.    | Extensiones del certificado .....  | 46        |
| 7.1.3.    | Identificadores de objeto de algoritmos .....                                  | 46        |
| 7.1.4.    | Formatos de nombres.....   | 46        |
| 7.1.5.    | Restricciones de nombres .....   | 46        |
| 7.1.6.    | Identificador de objeto de política de certificado.....                        | 47        |
| 7.1.7.    | Empleo de la extensión restricciones de política .....                         | 47        |
| 7.1.8.    | Sintaxis y semántica de los calificadores de política .....                    | 47        |
| 7.1.9.    | Tratamiento semántico para la extensión “certificate policy”.....              | 47        |
| 7.2.      | <i>Perfil de la CRL.....</i>   | <i>47</i> |
| 7.2.1.    | Número de versión.....   | 47        |
| 7.2.2.    | CRL y extensiones .....  | 47        |
| 7.3.      | <i>Perfil de OCSP.....</i>   | <i>48</i> |
| 7.3.1.    | Número de versión.....   | 48        |
| 7.3.2.    | Extensiones del OCSP .....   | 48        |
| <b>8.</b> | <b>Auditorías de cumplimiento .....</b>  | <b>48</b> |



|           |  |           |
|-----------|--|-----------|
| 8.1.      | <i>Frecuencia de las Auditorías</i> .....                          | 48        |
| 8.2.      | <i>Cualificación del auditor</i> .....                             | 49        |
| 8.3.      | <i>Relación del auditor con la empresa auditada</i> .....          | 49        |
| 8.4.      | <i>Elementos objetos de auditoría</i> .....                        | 49        |
| 8.5.      | <i>Toma de decisiones frente a detección de deficiencias</i> ..... | 50        |
| 8.6.      | <i>Comunicación de los resultados</i> .....                        | 50        |
| 8.7.      | <i>autoevaluación</i> .....  | 50        |
| <b>9.</b> | <b>Otros asuntos legales y de actividad</b> .....                  | <b>50</b> |
| 9.1.      | <i>Tarifas</i> .....   | 50        |
| 9.1.1.    | Tarifas de emisión o renovación de certificados.....               | 50        |
| 9.1.2.    | Tarifas de acceso a los certificados.....                          | 50        |
| 9.1.3.    | Tarifas de acceso a la información de estado o revocación.....     | 50        |
| 9.1.4.    | Tarifas para otros servicios.....                                  | 50        |
| 9.1.5.    | Política de reembolso.....   | 50        |
| 9.2.      | <i>Responsabilidad financiera</i> .....                            | 50        |
| 9.2.1.    | Seguro de responsabilidad civil.....                               | 51        |
| 9.2.2.    | Otros activos.....   | 51        |
| 9.2.3.    | Seguros y garantías para entidades finales.....                    | 51        |
| 9.3.      | <i>Confidencialidad de la información</i> .....                    | 51        |
| 9.3.1.    | Alcance de la información confidencial.....                        | 51        |
| 9.3.2.    | Información no incluida en el alcance.....                         | 51        |
| 9.3.3.    | Responsabilidad para proteger la información confidencial.....     | 51        |
| 9.4.      | <i>Protección de datos de carácter personal</i> .....              | 51        |
| 9.4.1.    | Plan de privacidad.....  | 51        |
| 9.4.2.    | Información tratada como privada.....                              | 51        |
| 9.4.3.    | Información no considerada privada.....                            | 51        |
| 9.4.4.    | Responsabilidad de proteger la información privada.....            | 51        |
| 9.4.5.    | Aviso y consentimiento para usar información privada.....          | 52        |
| 9.4.6.    | Divulgación conforme al proceso judicial o administrativo.....     | 52        |
| 9.4.7.    | Otras circunstancias de divulgación de información.....            | 52        |
| 9.5.      | <i>derechos de propiedad intelectual</i> .....                     | 52        |
| 9.6.      | <i>Obligaciones y garantías</i> .....                              | 52        |
| 9.6.1.    | Obligaciones de la AC.....   | 52        |
| 9.6.2.    | Obligaciones de la AR.....   | 52        |
| 9.6.3.    | Obligaciones del suscriptor y del firmante.....                    | 53        |
| 9.6.4.    | Obligaciones de las partes que confían.....                        | 54        |
| 9.6.5.    | Obligaciones de otros participantes.....                           | 54        |
| 9.7.      | <i>Renuncia de garantías</i> .....                                 | 54        |
| 9.8.      | <i>Limitaciones de responsabilidad</i> .....                       | 55        |
| 9.9.      | <i>Indemnizaciones</i> .....                                       | 55        |
| 9.9.1.    | Indemnización de la CA.....  | 55        |
| 9.9.2.    | Indemnización de los Suscriptores.....                             | 55        |
| 9.9.3.    | Indemnización de las partes que confían.....                       | 55        |



|         |   |    |
|---------|---|----|
| 9.10.   | <i>Periodo de validez de este documento</i> .....                             | 55 |
| 9.10.1. | Plazo .....   | 55 |
| 9.10.2. | Terminación.....  | 55 |
| 9.10.3. | Efectos de la finalización.....   | 56 |
| 9.11.   | <i>Notificaciones individuales y comunicación con los participantes</i> ..... | 56 |
| 9.12.   | <i>Modificaciones de este documento</i> .....                                 | 56 |
| 9.12.1. | Procedimiento para las modificaciones.....                                    | 56 |
| 9.12.2. | Periodo y mecanismo de notificación .....                                     | 56 |
| 9.12.3. | Circunstancias bajo las cuales debe cambiarse un OID .....                    | 56 |
| 9.13.   | <i>Reclamaciones y resolución de disputas</i> .....                           | 56 |
| 9.14.   | <i>Normativa de aplicación</i> .....  | 56 |
| 9.15.   | <i>Cumplimiento de la normativa aplicable</i> .....                           | 56 |
| 9.16.   | <i>Estipulaciones diversas</i> .....  | 56 |
| 9.16.1. | Acuerdo íntegro .....   | 56 |
| 9.16.2. | Asignación .....  | 56 |
| 9.16.3. | Severabilidad .....   | 57 |
| 9.16.4. | Cumplimiento .....  | 57 |
| 9.16.5. | Fuerza Mayor.....   | 57 |
| 9.17.   | <i>Otras estipulaciones</i> .....   | 57 |

### Índice de tablas

|  |    |
|--|----|
| Tabla 1 – Certificado de la AC FNMT raíz.....    | 13 |
| Tabla 2 – Certificado de la AC subordinada ..... | 13 |
| Tabla 3 – Perfil de la CRL.....                  | 47 |



## 1. INTRODUCCIÓN

1. 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, atribuye en el artículo 21 al Consejo General del Poder Judicial (en adelante CGPJ) el establecimiento de los sistemas de firma electrónica a jueces y magistrados.
2. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, consagró el derecho de los ciudadanos a relacionarse electrónicamente con las diferentes Administraciones Públicas. El marco jurídico resultante de la aprobación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, viene a sistematizar toda la regulación relativa al procedimiento administrativo, clarificando e integrando el contenido de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y de la citada Ley 11/2007, de 22 de junio. Así mismo, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, regula los sistemas de identificación y firma electrónicas utilizados en el ámbito de la Administración de Justicia.
3. El Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS), establece un marco jurídico general para el uso de las *Firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de Certificados para la autenticación de sitios web.*

### 1.1. OBJETO

4. El presente documento tiene por objeto la información pública de las condiciones y características de los servicios de confianza y, especialmente, los servicios de emisión de *Certificados* electrónicos por parte de la FNMT-RCM como *Prestador de Servicios de Confianza*, recogiendo, en particular las obligaciones y procedimientos que se compromete a cumplir en relación con la emisión de *Certificados de Carrera Judicial*, así como las obligaciones que se compromete a cumplir en relación con:
  - la gestión de los *Datos de creación y verificación de Firma* y de los *Certificados*, las condiciones aplicables a la solicitud, emisión, uso y extinción de la vigencia de los *Certificados* y sus *Datos de creación de Firma*, y en su caso, la existencia de procedimientos de coordinación con los Registros Públicos correspondientes que permitan el intercambio de información de manera inmediata y confidencial sobre la vigencia de los poderes indicados en los *Certificados* y que deban figurar preceptivamente inscritos en dichos registros
  - la prestación del servicio de consulta del estado de validez de los *Certificados*.
5. Además, en el presente documento se recogen, bien directamente o con referencias a la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM* de la que depende la presente Declaración, los detalles del régimen de



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

6. Los *Certificados* emitidos por la FNMT-RCM bajo las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* son *Certificados Cualificados*, conforme al citado Reglamento eIDAS, así como a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia y conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Estos *Certificados* cumplen con lo dispuesto en el artículo 23 del RD 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

## 1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

7. La *Declaración de Prácticas de Certificación* de la FNMT-RCM como *Prestador de Servicios de Confianza* está estructurada, de un lado, por la parte común de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)* de la FNMT-RCM, pues existen niveles de actuación análogos para todos los servicios de confianza de la Entidad y, de otro lado, por los apartados específicos del presente documento de *Políticas de Certificación y Prácticas de Certificación Particulares*. No obstante lo anterior, la *Ley de Emisión* de cada tipo de *Certificado* o grupo de *Certificados* podrá establecer características especiales aplicables a los órganos, organismos, entidades y personal usuarios de los servicios de confianza de la FNMT-RCM.
8. De acuerdo con lo anterior, la estructura de la *Declaración de Prácticas de Certificación de la FNMT-RCM* es la siguiente:
  - Por una parte, la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, que debe considerarse cuerpo principal de la *Declaración de Prácticas de Certificación* en el que se describe el régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica*, los controles de seguridad aplicados a los procedimientos e instalaciones de la FNMT-RCM, en aquello que pueda ser publicado sin perjudicar la eficacia de los mismos, las normas de secreto y confidencialidad, así como cuestiones relativas a la propiedad de sus bienes y activos, a la protección de datos de carácter personal y demás cuestiones de tipo informativo general que deben ponerse a disposición del público, independientemente de su papel en la Comunidad Electrónica.
  - Y, por otra parte, para cada servicio de confianza o conjunto o grupo de *Certificados*, identificado y diferenciado del resto por su tipología y régimen particular o diferenciador, existe una *Política de Certificación* específica en la que se describen las obligaciones de las partes, los límites de uso de los *Certificados* y responsabilidades y unas *Prácticas de Certificación Particulares* que desarrollan los términos definidos en



la política correspondiente y otorgan prestaciones adicionales o específicas sobre las generales establecidas en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*.

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

- El presente documento representa, además, las *Políticas de Certificación y Prácticas de Certificación Particulares* para los siguientes *Certificados en el ámbito de las actuaciones jurisdiccionales*:

*i. Certificado de Carrera Judicial*

▪ *Certificado Centralizado de Carrera Judicial*

9. El presente documento se denomina “*Políticas y Prácticas de Certificación de Certificados de Carrera Judicial*”, y en adelante será citado en este documento y con el ámbito descrito en el mismo como “*Declaración de Prácticas y Políticas Particulares*” o por su acrónimo “*DPPP*”.
10. Las presentes *Políticas de Certificación y Prácticas de Certificación Particulares* forman parte de la *Declaración de Prácticas de Certificación* y tendrán prelación sobre lo dispuesto en el cuerpo principal de la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (DGPC)*.
11. En caso de que existiera contradicción entre el presente documento y lo dispuesto en la *Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica*, tendrá preferencia lo aquí articulado.
12. Adicionalmente para los *Certificados de Firma Centralizada* se atenderá a lo dispuesto en la *Política y Prácticas del servicio de firma en servidor* que establece el conjunto de reglas y procedimientos específicos seguidos por la FNMT-RCM para la prestación de su servicio de firma electrónica en servidor.
13. En el presente documento se incluyen las siguientes *Políticas de Certificación* identificadas de la siguiente forma:

**Nombre:** Política de Certificación de *Certificado Centralizado de Carrera Judicial*

Referencia / OID: 1.3.6.1.4.1.5734.3.17.8

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

Tipo de política Carrera Judicial: QSCD HSM. OID: 2.16.724.6.0.1.1.5

**Versión:** 1.0

**Fecha de aprobación:** 11/09/2024



**Localización:** <http://www.cert.fnmt.es/dpcs/>

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

**Localización:** <http://www.cert.fnmt.es/dpcs/>

14. El *Certificado de Carrera Judicial*, es el *Certificado de Firma Electrónica* emitido por la FNMT-RCM que vincula al *Firmante* con unos *Datos de verificación de Firma* y confirma, de forma conjunta:
- la identidad del *Firmante* (persona física que actúa como *miembro de la Carrera Judicial*), incluyendo en su caso, su número de identificación profesional, categoría profesional, órgano en el que presta servicio y/o condición de autorizado, y
  - la identidad del *Suscriptor* del *Certificado*, donde el *Firmante* ejerce sus competencias, presta sus servicios, o desarrolla su actividad.
15. El *Certificado Centralizado de Carrera Judicial* está orientado a la realización de firmas a distancia o en servidor, esto es, la generación de las *Claves pública y privada* no son generadas directamente en el navegador de Internet del *Firmante* o en otro dispositivo en su poder, y tampoco se descarga su *Certificado*, sino que se generan y se almacenan en un dispositivo cualificado de creación de firma de la FNMT-RCM. Asimismo, la firma electrónica se realiza de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del *Firmante* al que se le ha expedido el *Certificado*.
16. La FNMT-RCM interpretará, registrará, mantendrá, y publicará los procedimientos referidos en este apartado, pudiendo además recibir comunicaciones de los interesados sobre estos asuntos a través de la información de contacto expresada en el apartado 1.5.2 Datos de contacto del presente documento.

### 1.3. PARTES INTERVINIENTES

17. Las partes que intervienen en la gestión y uso de los *Servicios de Confianza* descritos en la presente *DPPP* son las siguientes:
1. Autoridad de Certificación
  2. Autoridad de Registro
  3. *Firmantes*
  4. *Suscriptores* de los *Certificados*
  5. Partes que confían
  6. Otros participantes

#### 1.3.1. Autoridad de Certificación

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



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

**Tabla 1 – Certificado de la AC FNMT raíz**

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

- b) Autoridad de Certificación subordinada: expide los Certificados de entidad final objeto de la presente *DPPP*. El *Certificado* de dicha Autoridad viene identificado por la siguiente información:

**Tabla 2 – Certificado de la AC subordinada**

| Certificado de la AC subordinada |  |
|----------------------------------|--|
| Sujeto                           | CN = AC Sector Público, serialNumber = Q2826004J, OU = CERES, O = FNMT-RCM, C = ES |
| Emisor                           | OU = AC RAIZ FNMT-RCM, O = FNMT-RCM, C = ES  |
| Número de serie (hex)            | 34 81 60 C5 1F 5E DB CB 5D DF 89 CA B4 57 33 92                                    |



| Certificado de la AC subordinada |   |
|----------------------------------|---|
| Validez                          | No antes: 28 de noviembre de 2019 No después: 28 de noviembre de 2029 |
| Longitud clave pública           | RSA 4096 bits   |
| Algoritmo de firma               | RSA – SHA256  |
| Identificador de clave           | E7:04:EE:70:91:11:92:44:F9:0E:92:8F:56:43:1E:07:1D:BF:04:9C           |

### 1.3.2. Autoridad de Registro

19. La Autoridad de Registro realiza las tareas de identificación del solicitante, *miembro de la Carrera Judicial*, así como la comprobación de la documentación acreditativa de las circunstancias que constan en los mismos, la validación y la aprobación de las solicitudes de emisión, revocación y, en su caso, la renovación de dichos *Certificados*.
20. Podrán actuar como entidades de registro de FNMT-RCM aquellas Oficinas de Registro designadas por el órgano, organismo o entidad *Suscriptora* del *Certificado* con las que ésta suscriba el correspondiente instrumento legal para cubrir dicha finalidad.

### 1.3.3. Firmantes

21. Los *Firmantes* son las personas físicas que actúan como *miembros de la Carrera Judicial*. Corresponde al Firmante mantener bajo su uso exclusivo los *Datos de creación de firma* asociados a dicho *Certificado*. Es el titular y responsable del uso del *Certificado* que posee el control exclusivo y la capacidad de decisión sobre el propio certificado.

### 1.3.4. Suscriptores de los certificados

22. El *Suscriptor* de los *Certificados de Carrera Judicial* es la persona jurídica, órgano u organismo público destinatario de las actividades de la FNMT-RCM como *Prestador de Servicios de Certificación*, que suscribe los términos y condiciones del servicio y se referencia en el Sujeto en el Certificado.

### 1.3.5. Partes que confían

23. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del *Firmante / Suscriptor*, que reciben y / o usan *Certificados* expedidos por la FNMT-RCM y, como tales,



les es de aplicación lo establecido por la presente *DPPP* cuando deciden confiar efectivamente en tales *Certificados*.

### 1.3.6. Otros participantes

24. No estipulado.

## 1.4. USO DE LOS CERTIFICADOS

### 1.4.1. Usos permitidos de los certificados

25. Los *Certificados de Carrera Judicial*, a los que aplica esta *DPPP* son *Certificados Cualificados* conforme al Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93 (Reglamento eIDAS) y de conformidad con los requisitos establecidos en los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates”, ETSI EN 319 412-2 “Certificate profile for certificates issued to natural persons” .

26. Los *Certificados de Carrera Judicial* emitidos bajo esta *Política de Certificación* son expedidos a miembros de Carrera Judicial. Estos *Certificados* son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia y el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

27. El ámbito de aplicación de los *Certificados* expedidos bajo las Políticas identificadas con la denominación *Certificados Centralizados de Carrera Judicial* a los efectos de identificación como miembro de la Carrera Judicial y pueden utilizarse para la realización de las autenticaciones y firmas electrónicas requeridas, exclusivamente, en la *Actuación Jurisdiccional*.

### 1.4.2. Restricciones en el uso de los certificados

28. Constituyen límites de uso de los *Certificados de Carrera Judicial* las diferentes competencias y funciones propias de *Firmante* de los *Certificados*, de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización como miembro de la *Carrera Judicial*. La FNMT-RCM y la Administración, organismos y entidades públicas podrán fijar en los acuerdos o convenios, a través del documento de relación correspondiente o, si fuera procedente, en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.

29. Constituyen límites de uso de los *Certificados de Carrera Judicial*, de conformidad con la Ley 40/2015, y con la Ley 18/2011, de 5 de julio, para realización de las autenticaciones y firmas dentro del ejercicio de la competencia y en el ámbito de la *Actuación Jurisdiccional*.

30. FNMT-RCM no tendrá control sobre las actuaciones y usos de los *Certificados de Carrera Judicial* y la *Clave privada* que se realicen por los *miembros de Carrera Judicial*, por lo que la FNMT-RCM quedará exonerada de responsabilidad a efectos de tales usos, así como de las



- consecuencias y efectos que pudieran producirse en el marco de reclamaciones o, en su caso, de posibles responsabilidades patrimoniales llevadas a cabo por terceros.
31. En cuanto a las actividades del personal de las *Oficinas de Registro*, la FNMT – RCM quedará sujeta a las obligaciones y responsabilidades derivadas de la legislación en materia de firma electrónica, sin perjuicio de las especialidades contenidas en el artículo 11 del RD 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas. Para poder usar los *Certificados* de forma diligente, se deberá previamente formar parte de la *Comunidad Electrónica* y, la Administración actuante, adquirir la condición de *Suscriptor*.
32. La FNMT-RCM y la Administración, organismos y entidades podrán fijar en los acuerdos o convenios, o a través del documento de relación correspondiente o, si fuera procedente en la *Ley de Emisión* de estos *Certificados*, otros límites adicionales.
33. En cualquier caso, si un tercero desea confiar en la *Firma* realizada con uno de estos *Certificados* sin acceder al *Servicio de información sobre el estado de los Certificados* emitidos bajo esta *Política de Certificación*, no se obtendrá cobertura de las presentes *Políticas de Certificación y Prácticas de Certificación Particulares*, y se carecerá de legitimidad alguna para reclamar o emprender acciones legales contra la FNMT-RCM por daños, perjuicios o conflictos provenientes del uso o confianza en un *Certificado*.
34. Además, incluso dentro del ámbito de la *Comunidad Electrónica*, no se podrá emplear este tipo de *Certificados* para:
- Firmar o sellar otro *Certificado*, salvo supuestos expresamente autorizados previamente.
  - Usos particulares o privados.
  - Usos para relacionarse con las Administraciones, salvo cuando éstas lo admitan.
  - Firmar o sellar software o componentes.
  - Generar sellos de tiempo para procedimientos de *Fechado electrónico*.
  - Prestar servicios a título gratuito u oneroso, salvo supuestos expresamente autorizados previamente, como por ejemplo serían a título enunciativo:
    - Prestar servicios de *OCSP*.
    - Generar *Listas de Revocación*.
    - Prestar servicios de notificación
  - Cualquier uso que exceda de la finalidad de este tipo de *Certificados* sin la autorización previa de la FNMT-RCM.



## 1.5. ADMINISTRACIÓN DE POLÍTICAS

### 1.5.1. Entidad responsable

35. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, con NIF Q2826004-J, es la Autoridad de Certificación que expide los *Certificados* a los que aplica esta *Declaración de Prácticas y Políticas de Certificación*.

### 1.5.2. Datos de contacto

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

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

Dirección de Sistemas de Información - Departamento CERES

C/ Jorge Juan, 106

28071 – MADRID

E-mail: [ceres@fnmt.es](mailto:ceres@fnmt.es)

Teléfono: +34 91 740 69 82

37. Para informar problemas de seguridad relacionados con un certificado, tales como sospecha de compromiso clave, uso indebido o fraude, envíenos un informe de incidencia sobre certificado (CPR) a la cuenta de correo electrónico: [incidentes.ceres@fnmt.es](mailto:incidentes.ceres@fnmt.es).

### 1.5.3. Responsables de adecuación de la DPC

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

### 1.5.4. Procedimiento de aprobación de la DPC

39. La FNMT-RCM a través de su Comité de Gestión del *Prestador de Servicios de Confianza*, vela por el cumplimiento de la presente *Declaración de Políticas y Prácticas de Certificación particulares*, las aprueba, revisa y actualiza anualmente para mantenerlas acorde a la última versión de los referidos requisitos, incrementando el número de versión y agregando una entrada de registro de cambios con fecha, incluso si no se realizaron otros cambios en el documento.



## 1.6. DEFINICIONES Y ACRÓNIMOS

### 1.6.1. Definiciones

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

- *Actuación Jurisdiccional*: Ejercicio de la potestad jurisdiccional según lo establecido en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y demás normativa vigente.
- *Certificado de Firma Centralizada*: Es el *Certificado de Firma Electrónica* orientado a la realización de firmas en remoto o en servidor. Esto significa que la generación de las *Claves pública y privada* se generan y almacenan en un entorno seguro perteneciente a la FNMT-RCM, garantizándose en todo momento el control exclusivo del uso de dichas *Claves* por parte del *Firmante*. A efectos de la presente *DPPP* son *Certificados de Firma Centralizada*:
  - *Certificado Centralizado de Carrera Judicial*
- *Certificado Centralizado de Carrera Judicial*: es el *Certificado de Firma Electrónica Centralizada* cuyo *Firmante* será siempre miembro de la Carrera Judicial y que vincula los datos de validación de una persona física y confirma el número de identificación profesional otorgado por el Consejo de Poder Judicial como medio de identificación y firma de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
- *Código de Activación*: es una clave alfanumérica utilizada para validar y activar una cuenta en el Portal de Gestión de Identidades.
- *Declaración de Prácticas y Políticas Particulares (DPPP)*: *DPC* particular que aplica a la expedición de un conjunto determinado de *Certificados* expedidos por la FNMT-RCM bajo las condiciones particulares recogidas en dicha Declaración, y que le son de aplicación las Políticas particulares definidas en la misma.
- *Dispositivo cualificado de creación de firma (QSCD)*: dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014
- *Firmante*: *Persona física que actúa como miembro de la Carrera Judicial* y hace uso de sus *Datos de creación de firma*.
- *Organismo de supervisión*: organismo designado por un Estado miembro como responsable de las funciones de supervisión en materia de prestación de servicios de confianza, de conformidad con el artículo 17 del Reglamento eIDAS.
- *Miembro de la Carrera Judicial*: De conformidad con la Ley Orgánica 6/1985, del 1 de Julio del Poder Judicial, los Jueces y Magistrados profesionales formarán la Carrera Judicial. La Carrera Judicial consta de tres categorías: Magistrado del Tribunal Supremo, Magistrado y Juez.



- *Política y Prácticas del servicio de firma en servidor*: Documento que establece el conjunto de reglas y procedimientos específicos seguidos por la FNMT-RCM para la prestación de su servicio de firma electrónica en servidor
- *Responsable de Operaciones de Registro*: Persona física nombrada por el representante de la Administración pública, organismo público o entidad de derecho público, bajo cuya responsabilidad se realizan las tareas asignadas a la *Oficina de Registro*, con las obligaciones y responsabilidades asignadas en las presentes *Políticas y Prácticas de Certificación Particulares*.
- *Suscriptor*: La administración pública, órgano, organismo público o entidad de derecho público.

### 1.6.2. Acrónimos

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

**AC**: Autoridad de Certificación

**AR**: Autoridad de Registro

**ARL**: Lista de Revocación de Autoridades de Certificación

**CGPJ**: Consejo General del Poder Judicial

**CN**: Common Name (Nombre común)

**CRL**: Lista de *Certificados* revocados

**DN**: Distinguished Name (Nombre distintivo)

**DPC**: Declaración de Prácticas de Certificación

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

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

**ETSI**: European Telecommunications Standards Institute

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

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

**NCP**: Política de *Certificado* Normalizado

**NCP+**: Política de *Certificado* Normalizado Extendida

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

**OID**: Identificador de Objeto (Object Identifier)

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

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

**SIGOC**: Sistema de Información de Gestión de Órganos Judiciales y Carrera Judicial.



**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 REPOSITARIOS

### 2.1. REPOSITORIO

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

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

### 2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

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

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

### 2.3. FRECUENCIA DE PUBLICACIÓN

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

45. En cuanto a la frecuencia de publicación de CRL, se define en el apartado “4.9.7 Características adicionales. Frecuencia de publicación”.

### 2.4. CONTROL DE ACCESO A LOS REPOSITARIOS

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

## 3. IDENTIFICACIÓN Y AUTENTICACIÓN

### 3.1. NOMBRES

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



### 3.1.1. Tipos de nombres

48. Los *Certificados* electrónicos de entidad final objeto de la presente *DPPP* contienen un nombre distintivo (*DN*) en el campo Subject Name, que se componen según se describe en la información relativa al perfil del *Certificado*.
49. En el procedimiento de acreditación de la identidad, como paso previo a la expedición de un *Certificado de Carrera Judicial*, la FNMT-RCM, a través de la *Oficina de Registro*, constatará la verdadera identidad del *Firmante* y conservará la documentación que la acredite.

### 3.1.2. Significado de los nombres

50. Todos los nombres distintivos (*DN*) del campo Subject Name son significativos. La descripción de los atributos asociados al *Suscriptor* del *Certificado* es legible por humanos (véase el apartado 7.1.4 Formato de nombres del presente documento).
51. El campo Common Name de los *Certificados de Carrera Judicial* define al miembro de la Carrera Judicial al que se le ha expedido el *Certificado*.

### 3.1.3. Seudónimos

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

### 3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

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

### 3.1.5. Unicidad de los nombres

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

### 3.1.6. Reconocimiento y autenticación de marcas registradas

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



### 3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

#### 3.2.1. Métodos para probar la posesión de la clave privada

56. Para la expedición de los *Certificados Centralizados* se requerirá que el *Solicitante, miembro de la Carrera Judicial*, genere las *Claves pública y privada* en el sistema de la FNMT-RCM, después de haber sido registrado en el mismo y una vez validada dicha generación por parte de la *Oficina de Registro*, tras el proceso de acreditación de la identidad del citado *Solicitante* y recabada su voluntad.
57. Para los *Certificados Centralizados* después de informar al *Solicitante* que se le va a expedir su *Certificado*, el sistema genera la pareja de *Claves*, de forma que la *Clave privada* queda almacenada y protegida, garantizando su uso bajo el control exclusivo de los *miembros de la Carrera Judicial*.

#### 3.2.2. Autenticación de la identidad de la organización

58. Con carácter previo al establecimiento de cualquier relación institucional con los *Suscriptores*, la FNMT-RCM informa, a través de los medios y direcciones web citadas en estas *Prácticas de Certificación Particulares* y, subsidiariamente, en la *DGPC*, acerca de las condiciones del servicio, así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los *Certificados* por ella emitidos en su labor como *Prestador de Servicios de Confianza*.
59. Las actividades de comprobación de la identidad de los miembros de Carrera Judicial, *Solicitantes* de los *Certificados de Carrera Judicial*, serán realizadas por el personal autorizado de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión. Garantizando la identidad de la Administración, *Suscriptora* del *Certificado*.
60. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

#### 3.2.3. Autenticación de la identidad de la persona física solicitante

61. Este certificado se podrá emitir para todos los *miembros de la carrera judicial* compuesta por Jueces/zas, Magistrados/as y Magistrados/as del Tribunal Supremo. Así mismo también se podrá otorgar el certificado a Jueces/zas Sustitutos/as y Magistrados/as Suplentes en los periodos en los que sean nombrados.
62. Se hace constar que la FNMT-RCM, en función de la relación de *miembros de carrera judicial* remitida por la Administración, organismos o entidad pública, considerará, bajo responsabilidad de los correspondientes órganos, organismos y/o entidades, que actuarán a través de las *Oficinas de Registro*, que este personal se encuentra con su cargo vigente, que su número de Identificación Profesional, empleo o autorización es auténtico y está en vigor y, por tanto, habilitados para obtener y usar los *Certificados de Carrera Judicial*. FNMT-RCM, no tendrá, en este tipo de *Certificado*, la responsabilidad de comprobar el cargo o empleo del citado personal, así como que estos requisitos se mantienen durante toda la vida del *Certificado*, al no ostentar, la FNMT-RCM, relación jurídica funcionarial, administrativa o laboral con tal personal, más allá del documento de condiciones de utilización o, en su caso,



contrato de emisión, cuyo efecto es estrictamente instrumental para el desempeño de las funciones propias del cargo.

63. Estos *Certificados* son emitidos con la intervención del Consejo General de Poder Judicial, que tiene la capacidad de certificar la calidad de *miembro de la Carrera Judicial* de la persona identificada en el certificado y asignar el número de identificación profesional, único e intransferible a cada miembro de la Carrera Judicial.
64. Las actividades de comprobación anteriores serán realizadas por los responsables de las *Oficinas de Registro* implantadas por el órgano, organismo o entidad de la Administración Pública en cuestión, y que se corresponde, en cada caso, con el organismo o entidad donde el profesional judicial ejerce sus funciones. Por tanto y a estos efectos las *Oficinas de Registro* no serán autoridades delegadas o dependientes de la FNMT-RCM.

#### 3.2.3.1. Comprobación directa mediante presencia física

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

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

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

#### 3.2.4. Información no verificada del Suscriptor

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

#### 3.2.5. Validación de la autorización

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



### 3.2.6. Criterios de interoperación

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

### 3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES

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

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

#### 3.3.1. Renovación rutinaria

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

#### 3.3.2. Renovación después de una revocación

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

### 3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

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

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

## 4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

### 4.1. SOLICITUD DE CERTIFICADOS

#### 4.1.1. Quién puede solicitar un Certificado

76. El Solicitante de *Certificados de Carrera Judicial* solo puede ser miembro de la Carrera Judicial, compuesta por Jueces/zas, Magistrados/as y Magistrados/as del Tribunal Supremo. Así mismo también se podrá solicitar por Jueces/zas Sustitutos/as y Magistrados/as Suplentes en los periodos en los que sean nombrados.

#### 4.1.2. Proceso de registro y responsabilidades

77. El Solicitante de *Certificados* a través de la aplicación web de solicitud de *Certificados* desarrollada a tal efecto, deberá aceptar las condiciones de uso del *Certificado* e introducir



sus datos identificativos, tales como el NIF, primer apellido, entre otros y su dirección de correo electrónico a la que se enviará un código de solicitud.

78. La FNMT-RCM, tras recibir esta información, comprobará la validez de la información de la solicitud firmada, así como el tamaño de las claves generadas.
79. El apartado 9.8 “Responsabilidades” del presente documento establece las responsabilidades de las partes en este proceso.

## 4.2. PROCEDIMIENTO DE SOLICITUD DE CERTIFICADOS

### 4.2.1. Realización de las funciones de identificación y autenticación

80. Para los *Certificados de Carrera Judicial*, el *Solicitante* aportará los datos que se le requieran, acreditará su identidad personal y su condición de *miembro de la Carrera Judicial*. La FNMT-RCM admitirá, en todo caso, la función e informe que realice la *Oficina de Registro* designada por la Administración.
81. En el caso de *Certificados Centralizados* durante el proceso de acreditación de la identidad, el *Solicitante* suscribirá las condiciones de uso del *Certificado*, y se le dotará de unas credenciales de identificación y configurará un *Código de Activación*.
82. La FNMT-RCM, podrá acordar con las Administraciones, organismos y entidades públicas que así lo soliciten, la creación de Oficinas de Registro delegadas, con el fin de centralizar la realización de los procedimientos de registro con destino a otras Administraciones, vinculadas o dependientes, que no dispongan de medios suficientes para hacerlo en aplicación de las leyes sobre racionalización del gasto.

### 4.2.2. Aprobación o rechazo de la solicitud del certificado

83. Para los *Certificados Centralizados* una vez confirmados los datos, el *Solicitante* queda registrado en el sistema de la FNMT-RCM para dotarle de sus credenciales de identidad completas. La generación de las claves se producirá una vez que el *Firmante* configure la contraseña de firma que protegerá las claves, y solicite la generación de su identidad de firma. Estas acciones se llevarán a cabo accediendo con un nivel de aseguramiento alto a la aplicación de solicitud del *Certificado* (Portal de Gestión de Identidades).
84. La transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.
85. La FNMT-RCM recabará de los *Solicitantes* aquella información recibida de la *Oficina de Registro*, que sea necesaria para la expedición de los *Certificados* y para la comprobación de la identidad, almacenando la información exigida por la legislación de firma electrónica durante el periodo de quince (15) años tratándola con la debida diligencia para el cumplimiento de la legislación nacional vigente en materia de protección de datos de carácter personal.
86. Los datos personales y su tratamiento quedarán sometidos a la legislación específica.



#### 4.2.3. Tiempo en procesar la solicitud

87. La solicitud aprobada de los *Certificados Centralizados de Carrera Judicial* es procesada automáticamente por el sistema, por lo que no hay establecido un tiempo para este proceso.

#### 4.3. EMISIÓN DEL CERTIFICADO

##### 4.3.1. Acciones de la AC durante la emisión

88. Una vez recibidos en la FNMT-RCM los datos personales del *Solicitante*, la información que describe su relación con *el CGPJ y/o sus componentes dependientes*, así como el código de solicitud obtenido en la fase de solicitud, se procederá a la emisión del *Certificado*.

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

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

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

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

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

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

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

El atributo CN contiene los datos de identificación de los *miembros de Carrera Judicial* conforme al perfil del *Certificado* que corresponda.

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

93. El formato de los *Certificados*, expedidos por la FNMT-RCM bajo la presente *Política de Certificación*, en consonancia con la norma UIT-T X.509 versión 3 y de acuerdo con la normativa legalmente aplicable en materia de *Certificados Cualificados*, puede consultarse en la página <http://www.cert.fnmt.es/dpcs/>
94. En el proceso de emisión de los *Certificados de Carrera Judicial en QSCD*, se comprobará que el dispositivo empleado para la generación de claves de autenticación y firma es un *Dispositivo cualificado de creación de firma* conforme al Reglamento eIDAS.
95. En el proceso de emisión de los *Certificados Centralizados* se requiere que el *Solicitante* se identifique ante el sistema con las credenciales recibidas más un segundo factor de autenticación que será remitido a su dirección de correo electrónico<sup>1</sup> y, una vez verificada su identidad, deberá solicitar expresamente la emisión de su *Certificado Centralizado*. De esta forma, la infraestructura vincula de forma segura los datos de identificación proporcionados por el *Solicitante*, según se ha descrito en el apartado “4.1.2 Proceso de registro” del presente documento, con el proceso de generación de su *Certificado*.
96. En ese momento, el sistema generará en un HSM protegido las *Claves pública y privada*, y expedirá a los *miembros de Carrera Judicial* el *Certificado Centralizado* solicitado. Así mismo, el sistema requiere que el *Solicitante* establezca su contraseña de firma que le será requerida para realizar las operaciones que usen su *Clave privada*. Esta contraseña no es conocida (ni almacenada) en ningún momento por el sistema de la FNMT-RCM.

#### 4.3.2. Notificación de la emisión

97. Una vez emitido el *Certificado Centralizado de Carrera Judicial*, la FNMT-RCM informará los *miembros de Carrera Judicial* sobre la disponibilidad de *Certificado* para su descarga.

#### 4.4. ACEPTACIÓN DEL CERTIFICADO

##### 4.4.1. Proceso de aceptación

98. En el proceso de solicitud del *Certificado*, los *miembros de Carrera Judicial* aceptan las condiciones de uso y expresa su voluntad de obtener el *Certificado*, como requisitos necesarios para la generación del mismo.

##### 4.4.2. Publicación del certificado por la AC

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

---

<sup>1</sup> La FNMT-RCM podrá utilizar otros medios de comunicación para transmitir este segundo factor de autenticación, previa autorización del *Solicitante*, como por ejemplo el uso de teléfonos móviles cuyo número haya sido previamente acreditado.



#### 4.4.3. Notificación de la emisión a otras entidades

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

#### 4.5. PAR DE CLAVES Y USO DEL CERTIFICADO

##### 4.5.1. Clave privada y uso del certificado

101. La FNMT-RCM genera y almacena las Claves Privadas asociadas a los *Certificados de Firma Centralizada*.

102. Estos *Certificados* son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

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

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

#### 4.6. RENOVACIÓN DEL CERTIFICADO

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

##### 4.6.1. Circunstancias para la renovación del certificado

105. 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

106. 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

107. 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

108. 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

109. 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

110. 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

111. 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

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

#### 4.7.1. Circunstancias para la renovación con regeneración de claves

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

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

#### 4.7.2. Quién puede solicitar la renovación con regeneración de claves

114. 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

115. 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

116. 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

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

#### 4.7.6. Publicación del certificado renovado

118. 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**

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

**4.8. MODIFICACIÓN DEL CERTIFICADO**

120. 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**

121. No se estipula la modificación.

**4.8.2. Quién puede solicitar la modificación del certificado**

122. No se estipula la modificación.

**4.8.3. Procesamiento de solicitudes de modificación del certificado**

123. No se estipula la modificación.

**4.8.4. Notificación de la modificación del certificado**

124. No se estipula la modificación.

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

125. No se estipula la modificación.

**4.8.6. Publicación del certificado modificado**

126. No se estipula la modificación.

**4.8.7. Notificación de la modificación del certificado a otras entidades**

127. No se estipula la modificación.

**4.9. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO**

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

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

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



- c) Revocación del *Certificado* por cualquiera de las causas recogidas en el presente documento.
129. 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*.
130. La FNMT-RCM pone a disposición de los Suscriptores, terceros que confían, proveedores de software y terceras partes una vía de comunicación a través de la sede electrónica de la FNMT-RCM <https://www.sede.fnmt.gob.es/>

#### 4.9.1. Circunstancias para la revocación

##### 4.9.1.1 Circunstancias para la revocación del certificado del suscriptor

131. La solicitud de revocación de los *Certificados* podrá efectuarse durante el período de validez que consta en el *Certificado*.
132. Serán causas admitidas para la revocación de un *Certificado* las expuestas a continuación:
- La solicitud de revocación por parte de las personas autorizadas. En todo caso deberá dar lugar a esta solicitud:
    - La utilización por un tercero de la Clave Privada asociada al *Certificado*
    - La violación o puesta en peligro del secreto de los *Datos de Creación de Firma* o de la clave privada asociada al *Certificado*.
    - La no aceptación de las nuevas condiciones que puedan suponer la expedición de nuevas *Declaraciones de Prácticas y Políticas de Certificación*, durante el periodo de un mes tras su publicación.
  - Resolución judicial o administrativa que así lo ordene.
  - Extinción o disolución de la personalidad jurídica del *Suscriptor*
  - Fallecimiento o incapacidad sobrevenida, total o parcial, del *Firmante* o del representante del *Suscriptor*.
  - Inexactitudes en los datos aportados por el *Solicitante* para la obtención del *Certificado*, o alteración de los datos aportados para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado*, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
  - Contravención de una obligación sustancial de esta *Declaración de Prácticas y Políticas de Certificación* por parte del *Firmante* o del *Solicitante* del *Certificado* o por parte de una *Oficina de Registro* si, en este último caso, hubiese podido afectar al procedimiento de emisión del *Certificado*
  - Violación o puesta en peligro del secreto de los Datos de Creación de Firma o de la Clave Privada.

- h) Resolución del contrato suscrito entre el *Firmante* o el Suscriptor y la FNMT-RCM.
  - i) Contravención de una obligación sustancial de esta *Declaración de Prácticas y Políticas de Certificación* por parte de una *Oficina de Registro* si hubiese podido afectar al procedimiento de expedición del *Certificado*.
  - j) Cese en la actividad del *Prestador de Servicios de Confianza* salvo que la gestión de los *Certificados* electrónicos expedidos por aquél sea transferida a otro *Prestador de Servicios de Confianza*.
  - k) Cancelación de las credenciales de identificación del *Firmante* cuando sean *Certificados de Firma Centralizada*.
  - l) Pérdida de la certificación de *Dispositivo cualificado de creación de firma* QSCD, cuando sean *Certificados de Firma Centralizada*.
133. En ningún caso la FNMT-RCM asume obligación alguna de comprobar los extremos mencionados en las letras c) a e) del presente apartado, debiendo ser notificadas a esta entidad de forma fehaciente mediante entrega de los documentos e informaciones necesarias para verificarlo.
134. La FNMT-RCM únicamente será responsable de las consecuencias que se desprendan de no haber revocado un *Certificado* en los siguientes supuestos:
- Que la revocación se debiera haber efectuado por haberse extinguido el contrato suscrito con el *Suscriptor*
  - Que la revocación le haya sido solicitada a través de la *Oficina de Registro* correspondiente a la entidad u organismo *Suscriptor* siguiendo el procedimiento establecido para este tipo de *Certificados*
  - Que la solicitud de revocación o la causa que la motiva, le haya sido notificada mediante resolución judicial o administrativa.
  - Que en las causas c) a e) del presente apartado le sean acreditados dichos extremos fehacientemente, previa identificación del *Solicitante* de la revocación.
135. Las actuaciones constitutivas de delito o falta de las que no tenga conocimiento la FNMT-RCM que se realicen sobre los datos y/o *Certificado* y las inexactitudes sobre los datos o falta de diligencia en su comunicación a la FNMT-RCM, producirán la exoneración de responsabilidad de la FNMT-RCM.
136. La revocación de los *Certificados* implica, además de su extinción y la imposibilidad de seguir utilizando los *Datos de creación de firma* o claves privadas asociados, la finalización de la relación y régimen de uso de dicho *Certificado* y su *Clave privada* con la FNMT-RCM.

#### 4.9.1.2 Circunstancias para la revocación del certificado de la CA subordinada

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



#### 4.9.2. Quién puede solicitar la revocación

138. La revocación de un *Certificado* solamente podrá ser solicitada por:
- la *Autoridad de Certificación* y la *Autoridad de Registro*
  - el *Suscriptor* a través de su representante o persona autorizada, en la Oficina de Registro habilitada a tal efecto
  - en su caso, el *Firmante*, a través del teléfono habilitado para tal fin (previa identificación del Solicitante) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7, o bien a través de dicha Oficina de Registro.
139. La FNMT-RCM podrá revocar de oficio los *Certificados* en los supuestos recogidos en la presente *Declaración de Prácticas y Políticas de Certificación*.

#### 4.9.3. Procedimiento de solicitud de la revocación

140. La solicitud de revocación de los *Certificados de Carrera Judicial* podrá efectuarse durante el periodo de validez que consta en el *Certificado*.
141. El proceso de revocación puede realizarse de forma ininterrumpida 24x7, a través del Servicio de Revocación telefónica puesto a disposición de los usuarios para esta finalidad, asegurando la revocación del *Certificado* en un plazo inferior a 24h.
142. Durante la revocación telefónica, el solicitante de la revocación tendrá que confirmar los datos que se le soliciten, y aportar aquellos que sean imprescindibles para la validación de forma inequívoca de su capacidad para solicitar dicha revocación.
143. Adicionalmente, se puede solicitar la revocación de cualquier *Certificado* a través de la *Oficina de Registro*. Los datos personales y su tratamiento quedarán sometidos a la legislación específica. El proceso de revocación en la oficina de registro es el siguiente:
- Para los *Certificados Centralizados de Carrera Judicial*, el solicitante deberá presentarse en su *Oficina de Registro*, donde se acreditará su identidad, se validará su capacidad para revocar dicho *Certificado* y se consignará la causa de revocación. La Oficina enviará de forma telemática mediante la aplicación de registro los datos a la FNMT-RCM, y procederá a la revocación del *Certificado*.
144. Tan pronto la revocación sea efectiva, serán notificados a través de la dirección de correo electrónico:
- El *Firmante* y solicitante de la revocación cuando se trate de un *Certificado de Carrera Judicial*
145. Una vez que la FNMT-RCM ha procedido a la revocación del *Certificado*, se publicará en el *Directorio* seguro la correspondiente *Lista de Certificados Revocados*, conteniendo el número de serie del *Certificado* revocado, así como la fecha, hora y causa de revocación. Una vez que un *Certificado* ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.
146. Para informar de posibles compromisos de Claves Privada, uso indebido de certificados u otros tipos de fraude, conducta inapropiada o cualquier otro asunto relacionado con los



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

#### 4.9.4. Periodo de gracia de la solicitud de revocación

147. 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

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

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

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

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

#### 4.9.7. Frecuencia de generación de CRLs

150. Las *Listas de Revocación (CRL)* de los *Certificados Centralizados de Carrera Judicial* se emiten al menos cada 12 horas, o cuando se produce una revocación y tienen un periodo de validez de 24 horas. Las *CRL* de los *Certificados de Autoridad* se emiten cada 6 meses, o cuando se produce una revocación de una *Autoridad de Certificación* subordinada y tienen un periodo de validez de 6 meses.

#### 4.9.8. Periodo máximo de latencia de las CRLs

151. 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

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

#### 4.9.10. Requisitos de comprobación en línea de la revocación

153. La comprobación en línea del estado de revocación de los *Certificados Centralizados de Carrera Judicial* 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

154. No definidas.

#### 4.9.12. Requisitos especiales de revocación de claves comprometidas

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

#### 4.9.13. Circunstancias para la suspensión

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

#### 4.9.14. Quién puede solicitar la suspensión

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

#### 4.9.15. Procedimiento para la petición de la suspensión

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

#### 4.9.16. Límites sobre el periodo de suspensión

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

### 4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE LOS CERTIFICADOS

#### 4.10.1. Características operativas

160. La información relativa a la validación de los *Certificados* electrónicos objeto de la presente *DPPP* es accesible a través de los medios descritos en la *DGPC*.

#### 4.10.2. Disponibilidad del servicio

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



#### 4.10.3. Características opcionales

162. No estipuladas.

#### 4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

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

164. A los efectos enumerados anteriormente, se hace constar que la solicitud de emisión de un *Certificado Centralizado de Carrera Judicial* emitido por la FNMT-RCM cuando exista otro vigente a favor del mismo *Firmante* y mismo *Suscriptor*, y perteneciente a la misma *Ley de Emisión*, conllevará la revocación del primero obtenido.

#### 4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

##### 4.12.1. Prácticas y políticas de custodia y recuperación de claves

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

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

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

167. No estipulado.

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

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

##### 5.1. CONTROLES DE SEGURIDAD FÍSICA

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

###### 5.1.1. Ubicación de las instalaciones

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

###### 5.1.2. Acceso Físico

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

###### 5.1.3. Electricidad y Aire Acondicionado

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



**5.1.4. Exposición al agua**

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

**5.1.5. Prevención y Protección contra incendios**

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

**5.1.6. Almacenamiento de Soportes**

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

**5.1.7. Eliminación de Residuos**

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

**5.1.8. Copias de Seguridad fuera de las instalaciones**

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

**5.2. CONTROLES DE PROCEDIMIENTO**

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

**5.2.1. Roles de Confianza**

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

**5.2.2. Número de personas por tarea**

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

**5.2.3. Identificación y autenticación para cada rol**

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

**5.2.4. Roles que requieren segregación de funciones**

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

**5.3. CONTROLES DE PERSONAL**

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

**5.3.1. Conocimientos, cualificación, experiencia y requerimientos acreditativos**

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



**5.3.2. Procedimientos de verificación de antecedentes**

185. Véase el apartado correspondiente en la *DGPC*

**5.3.3. Requisitos de formación**

186. Véase el apartado correspondiente en la *DGPC*

**5.3.4. Requisitos y frecuencia de actuación formativa**

187. Véase el apartado correspondiente en la *DGPC*

**5.3.5. Secuencia y frecuencia de rotación laboral**

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

**5.3.6. Sanciones por acciones no autorizadas**

189. Véase el apartado correspondiente en la *DGPC*

**5.3.7. Requisitos de contratación de personal**

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

**5.3.8. Suministro de documentación al personal**

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

**5.4. PROCEDIMIENTOS DE AUDITORÍA**

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

**5.4.1. Tipos de eventos registrados**

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

**5.4.2. Frecuencia de procesamiento de registros**

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

**5.4.3. Periodo de conservación de los registros**

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

**5.4.4. Protección de los registros**

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



**5.4.5. Procedimientos de copias de seguridad de los registros auditados**

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

**5.4.6. Sistemas de recolección de registros**

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

**5.4.7. Notificación al sujeto causante de los eventos**

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

**5.4.8. Análisis de vulnerabilidades**

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

**5.5. ARCHIVADO DE REGISTROS**

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

**5.5.1. Tipos de registros archivados**

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

**5.5.2. Periodo de retención del archivo**

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

**5.5.3. Protección del archivo**

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

**5.5.4. Procedimientos de copia de respaldo del archivo**

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

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

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

**5.5.6. Sistema de archivo**

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

**5.5.7. Procedimientos para obtener y verificar la información archivada**

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



**5.6. CAMBIO DE CLAVES DE LA AC**

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

**5.7. GESTIÓN DE INCIDENTES Y VULNERABILIDADES**

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

**5.7.1. Gestión de incidentes y vulnerabilidades**

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

**5.7.2. Actuación ante datos y software corruptos**

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

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

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

**5.7.4. Continuidad de negocio después de un desastre**

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

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

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

**6. CONTROLES DE SEGURIDAD TÉCNICA**

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

**6.1. GENERACIÓN E INSTALACIÓN DE LAS CLAVES**

**6.1.1. Generación del par de claves**

*6.1.1.1 Generación del par de Claves de la CA*

217. En relación con la generación de las *Claves* de AC que la FNMT-RCM necesita para el desarrollo de su actividad como *Prestador de Servicios de Confianza*, véase el apartado correspondiente en la *DGPC*.

*6.1.1.2 Generación del par de Claves de la RA*

218. No estipulado



### 6.1.1.3 Generación del par de Claves de los Suscriptores

219. Las *Claves privadas* asociadas a los *Certificados de Carrera Judicial en QSCD* son generadas y custodiadas en un *Dispositivo cualificado de creación de firma* que cumple con los requisitos enumerados en el anexo II del Reglamento eIDAS.
220. Las *Claves privadas* asociadas a los *Certificados Centralizados de Carrera Judicial* son generadas y custodiadas por el módulo de activación de firma de la FNMT-RCM, de forma que el acceso a dichas *Claves* se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del *Firmante*.

### 6.1.2. Envío de la clave privada al suscriptor

221. No existe ninguna entrega de Clave privada en la emisión de los *Certificados* expedidos bajo las presentes *Políticas y Prácticas de Certificación*.
222. Las *Claves privadas* asociadas a los *Certificados Centralizados de Carrera Judicial* son generadas en un dispositivo de creación de firma bajo el control exclusivo del *Firmante*, donde quedarán custodiadas para su uso. No existiendo, tampoco en este caso, entrega de la *Clave privada* al *Firmante*.
223. En todo caso, si la FNMT-RCM o cualquiera de las oficinas de registro tuviera conocimiento de un acceso no autorizado a la *Clave privada* del *Firmante*, el *Certificado* asociado a dicha *Clave privada* será revocado.

### 6.1.3. Envío de la clave pública al emisor del certificado

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

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

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

### 6.1.5. Tamaños de claves y algoritmos utilizados

226. El algoritmo utilizado es RSA con SHA-256.
227. En cuanto al tamaño de las claves, dependiendo de cada caso, es:
- Claves de la AC FNMT raíz: 4096 bits.
  - Claves de la AC Sector Público Subordinada: 4096 bits.
  - Claves de los *Certificados Centralizados de Carrera Judicial*: 2048 bits.

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

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



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

- 229. Los *Certificados* FNMT incluyen la extensión Key Usage y, según el caso, Extended Key Usage, indicando los usos habilitados de las *Claves*.
- 230. El *Certificado* de la AC FNMT raíz tiene habilitados los usos de *Claves* para firmar/sellar los *Certificados* de las ACs FNMT Subordinadas y las ARLs.
- 231. El *Certificado* de la AC FNMT Subordinada que expide los *Certificados Centralizados de Carrera Judicial* tiene habilitado exclusivamente el uso para firmar/sellar *Certificados* de entidad final y CRLs.
- 232. Los *Certificados Centralizados de Carrera Judicial* tienen habilitado exclusivamente los usos de clave de cifrado, autenticación y firma

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

#### 6.2.1. Estándares para los módulos criptográficos

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

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

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

#### 6.2.3. Custodia de la clave privada

- 235. Las operaciones de copia, salvaguarda o recuperación de las *Claves privadas* de las Autoridades de Certificación de la FNMT-RCM se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.
- 236. Las *Claves privadas* asociadas a los *Certificados de Carrera Judicial en QSCD* son generadas y custodiadas en un *Dispositivo cualificado de creación de firma* que cumple con los requisitos enumerados en el anexo II del Reglamento eIDAS
- 237. En cuanto a las *Claves privadas* correspondientes a los *Certificados Centralizados de Carrera Judicial* expedidos a los usuarios finales (*Firmantes*), quedan custodiadas en los sistemas de la FNMT-RCM de forma que únicamente el *Firmante* puede acceder a su *Clave privada*. El acceso queda garantizado mediante el uso de sus credenciales de identificación y su contraseña de firma (únicamente conocidos por el *Firmante*), más un segundo factor de autenticación como es una contraseña de un solo uso.

#### 6.2.4. Copia de seguridad de la clave privada

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

#### 6.2.5. Archivado de la clave privada

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



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

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

#### 6.2.7. Almacenamiento de la clave privada en el módulo criptográfico

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

#### 6.2.8. Método de activación de la clave privada

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

243. Los mecanismos de activación y uso de las *Claves privadas* de la Autoridad de Certificación se basan en la segmentación de roles de gestión y operación que la FNMT-RCM tiene implementados con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultáneo M de N (2 de 5).

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

#### 6.2.9. Método de desactivación de la clave privada

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

#### 6.2.10. Método de destrucción de la clave privada

246. 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.

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

#### 6.2.11. Clasificación de los módulos criptográficos

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

### 6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

#### 6.3.1. Archivo de la clave pública

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



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

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

- *Certificado* de la AC FNMT raíz y su par de *Claves*: hasta el 1 de enero de 2030.
- El *Certificado* de la AC subordinada que expide los *Certificados de Carrera Judicial* y su par de *Claves*: hasta el 31 de diciembre de 2029.
- Los *Certificados Centralizados de Carrera Judicial* y su par de *Claves*: no superior a 4 años.

## 6.4. DATOS DE ACTIVACIÓN

### 6.4.1. Generación e instalación de datos de activación

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

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

### 6.4.2. Protección de datos de activación

253. Los datos de activación de las *Claves privadas* de la *Autoridad de Certificación* están protegidos, conforme al método descrito en el apartado “6.2.8 Método de activación de la *Clave privada*” del presente documento, con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultaneo M de N (2 de 5).

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

### 6.4.3. Otros aspectos de los datos de activación

255. No estipulados.

## 6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

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

### 6.5.1. Requisitos técnicos específicos de seguridad informática

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



**6.5.2. Evaluación del nivel de seguridad informática**

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

**6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA**

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

**6.6.1. Controles de desarrollo de sistemas**

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

**6.6.2. Controles de gestión de la seguridad**

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

**6.6.3. Controles de seguridad del ciclo de vida**

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

**6.7. CONTROLES DE SEGURIDAD DE RED**

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

**6.8. FUENTE DE TIEMPO**

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

**6.9. OTROS CONTROLES ADICIONALES**

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

**6.9.1. Control de la capacidad de prestación de los servicios**

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

**6.9.2. Control de desarrollo de sistemas y aplicaciones informáticas**

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

**7. PERFILES DE LOS CERTIFICADOS, CRLs Y OCSP**

**7.1. PERFIL DEL CERTIFICADO**

268. Los *Certificados de Carrera Judicial* son expedidos como “cualificados” de conformidad con los estándares europeos ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” y ETSI EN 319 412-2 “Certificate profile for certificates issued to natural persons”.



#### 7.1.1. Número de versión

269. Los *Certificados de Carrera Judicial* son conformes con el estándar X.509 versión 3.

#### 7.1.2. Extensiones del certificado

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

271. Todos los certificados emitidos bajo estas *políticas de certificación* contendrán una extensión no crítica, qcStatements, usando el qcStatement-2 predefinido en el RFC 3739, en el que todos los valores en semanticsInformation serán:

- semanticsIdentifier: id-etsi-qcs-semanticsId-Natural
- nameRegistrationAuthorities: <https://poderjudicial.es> (del tipo URI generalName)

#### 7.1.3. Identificadores de objeto de algoritmos

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

#### 7.1.4. Formatos de nombres

273. La codificación de los *Certificados de Carrera Judicial* 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.

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

275. La semántica de campo serialNumber será la siguiente:

JU:ES-JXXXXXXXXXR,

donde “xxxxxxxx” es un código personal, único e intransferible asignado a cada miembro de la carrera judicial por el Sistema de Información de Gestión de Órganos Judiciales y Carrera Judicial (SIGOC) y “R” un carácter de control.

#### 7.1.5. Restricciones de nombres

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

#### 7.1.6. Identificador de objeto de política de certificado

277. El identificador de objeto (OID) de la política del *Certificado Centralizado de Carrera Judicial* 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

278. La extensión “Policy Constrains” del *Certificado* raíz de la AC no es utilizado.

#### 7.1.8. Sintaxis y semántica de los calificadores de política

279. La extensión “Certificate Policies” incluye dos campos de “Policy Qualifiers”:

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

#### 7.1.9. Tratamiento semántico para la extensión “certificate policy”

280. La extensión “Certificate Policy” incluye el campo OID de política, que identifica la política asociada al *Certificado* por parte de la FNMT–RCM, así como los dos campos relacionados en el apartado anterior.

### 7.2. PERFIL DE LA CRL

#### 7.2.1. Número de versión

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

#### 7.2.2. CRL y extensiones

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

**Tabla 3 – Perfil de la CRL**

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



| Campos y extensiones                   | Valor  |
|--|--|
| Fecha de emisión                       | Tiempo UTC de emisión.   |
| Fecha de próxima actualización         | Fecha de emisión + 24 horas  |
| Identificador de la clave de Autoridad | Hash de la clave del emisor  |
| Punto de distribución                  | URLs del punto de distribución y ámbito de las CRLs  |
| ExpiredCertsOnCRL                      | NotBefore de la CA   |
| Certificados revocados                 | Lista de certificados revocados, conteniendo al menos para cada entrada, número de serie y fecha de revocación |

### 7.3. PERFIL DE OCSP

#### 7.3.1. Número de versión

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

#### 7.3.2. Extensiones del OCSP

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

## 8. AUDITORÍAS DE CUMPLIMIENTO

### 8.1. FRECUENCIA DE LAS AUDITORÍAS

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

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

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

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



- 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).
289. También se llevan a cabo análisis de riesgos, de acuerdo a lo dictado en el Sistema de Gestión de la Seguridad de la Información.
290. La *Autoridad de Certificación* que expide los *Certificados de Carrera Judicial* está sujeta a auditorías periódicas, de conformidad con el estándar europeo ETSI EN 319 401 “General Policy Requirements for Trust Service Providers”, ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates” y ETSI EN 319 412-2 “Certificate profile for certificates issued to natural persons”.
291. Las auditorías ETSI mencionadas en el apartado anterior se realizan anualmente por una empresa externa acreditada.
292. La frecuencia del resto de auditorías adicionales, será conforme a lo estipulado en la normativa vigente correspondiente.
- 8.2. CUALIFICACIÓN DEL AUDITOR**
293. Véase el apartado correspondiente en la *DGPC*.
- 8.3. RELACIÓN DEL AUDITOR CON LA EMPRESA AUDITADA**
294. Véase el apartado correspondiente en la *DGPC*.
- 8.4. ELEMENTOS OBJETOS DE AUDITORÍA**
295. Véase el apartado correspondiente en la *DGPC*.



**8.5. TOMA DE DECISIONES FRENTE A DETECCIÓN DE DEFICIENCIAS**

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

**8.6. COMUNICACIÓN DE LOS RESULTADOS**

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

**8.7. AUTOEVALUACIÓN**

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

**9. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD**

**9.1. TARIFAS**

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

**9.1.1. Tarifas de emisión o renovación de certificados**

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

**9.1.2. Tarifas de acceso a los certificados**

301. No estipulado.

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

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

**9.1.4. Tarifas para otros servicios**

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

**9.1.5. Política de reembolso**

304. 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**

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



**9.2.1. Seguro de responsabilidad civil**

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

**9.2.2. Otros activos**

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

**9.2.3. Seguros y garantías para entidades finales**

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

**9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN**

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

**9.3.1. Alcance de la información confidencial**

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

**9.3.2. Información no incluida en el alcance**

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

**9.3.3. Responsabilidad para proteger la información confidencial**

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

**9.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

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

**9.4.1. Plan de privacidad**

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

**9.4.2. Información tratada como privada**

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

**9.4.3. Información no considerada privada**

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

**9.4.4. Responsabilidad de proteger la información privada**

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



#### 9.4.5. Aviso y consentimiento para usar información privada

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

#### 9.4.6. Divulgación conforme al proceso judicial o administrativo

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

#### 9.4.7. Otras circunstancias de divulgación de información

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

### 9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

### 9.6. OBLIGACIONES Y GARANTÍAS

#### 9.6.1. Obligaciones de la AC

322. Las obligaciones y responsabilidades de la FNMT-RCM, como *Prestador de Servicios de Confianza*, con la persona asociada al *Certificado*, y que actúa como *Firmante*, y con el resto de miembros de la *Comunidad Electrónica*, quedarán determinadas, principalmente, por el documento relativo a las condiciones de utilización o el contrato de expedición del *Certificado*, y, subsidiariamente, por la presente *Declaración de Prácticas y Políticas de Certificación*.

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

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

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

#### 9.6.2. Obligaciones de la AR

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

- Comprobar fehacientemente los datos referidos a la identidad y a la condición de *miembro de la Carrera Judicial* del titular del certificado.
- El *Prestador de Servicios de Confianza*, a través del *Responsable de Operaciones de Registro* velará por el cumplimiento de los procedimientos aprobados por FNMT-RCM

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

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

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

### 9.6.3. Obligaciones del suscriptor y del firmante

328. De forma adicional a las obligaciones y responsabilidades de las partes enumeradas en la *DGPC*, los *miembros de Carrera Judicial*, como *Firmantes del Certificado*, tienen la obligación de:

- No utilizar el *Certificado* cuando alguno de los datos referidos al cargo, puesto de trabajo, empleo o cualquier otro sea inexacto o incorrecto o no refleje o caracterice su relación, con el órgano, organismo o entidad en la que presta sus servicios; o, existan razones de seguridad que así lo aconsejen.
- Utilizará de manera adecuada y custodiará de manera diligente el *Certificado*, según el propósito y función para el que ha sido expedido.
- Comunicar al *Responsable de Operaciones de Registro*, cualquiera de los hechos determinantes especificados en el apartado 4.9.1 de esta DPPP, con el fin de iniciar los trámites de revocación su *Certificado*.

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

- Conservar su confidencialidad, evitando comunicarlo a otras personas.
- Memorizarlo y no anotarlo en ningún documento físico ni electrónico.
- Cambiarlo en el momento en que tenga sospechas de que pueda ser conocido por otra persona.



- Notificar a la FNMT-RCM cualquier posible pérdida de control sobre su Clave privada, al objeto de revocar su *Certificado Centralizado* y sus Claves asociadas.
  - Abstenerse de escoger una contraseña fácilmente deducible de sus datos personales o predecibles (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones del mismo carácter, etc.).
  - Seguir la política de seguridad de la FNMT-RCM en relación con la composición de la contraseña, periodicidad de modificación del mismo, etc.
  - Las firmas electrónicas se crean exclusivamente haciendo uso del *QSCD* que el *PSC* le facilite en cada caso.
330. Será responsabilidad tanto del *Firmante* como del Suscriptor, 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.
331. En todo caso, el *Firmante* no usará los *Datos de creación de firma* o claves privadas, asociados a su *Certificado* en los casos en los que éste haya expirado su periodo de vigencia, o los *Datos de Creación de Firma* del Prestador puedan estar amenazados y/o comprometidos y así se haya comunicado por el Prestador o, en su caso, el *Firmante* conociera, sospechara o hubiera tenido noticia de estas circunstancias. Si el *Firmante* contraviniera esta obligación, será responsable de las consecuencias de los actos, documentos o transacciones firmadas en estas condiciones, así como de los costes, daños y perjuicios que pudieran derivarse, para la FNMT-RCM o para terceros, en caso de utilizar el *Certificado* más allá de su periodo de vigencia.
332. Asimismo, será el *Firmante* quien deba responder ante los miembros de la *Comunidad electrónica* y demás *Entidades usuarias* o, en su caso, ante terceros del uso indebido del *Certificado*, o actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros. Será responsabilidad del *Firmante* el uso que realice de su *Certificado*, en caso de que el *Prestador de Servicios de Confianza* haya cesado en la actividad como Entidad emisora de *Certificados* y no se hubiera producido la subrogación prevista en la ley.
333. El Suscriptor debe responder, en todo caso, ante la FNMT-RCM, las Entidades usuarias y, en su caso, ante terceros, de la falsedad o errores de las manifestaciones en recogidas en el *Certificado* durante el proceso de solicitud, y de los actos u omisiones que provoquen daños y perjuicios a la FNMT-RCM o a terceros.

#### 9.6.4. Obligaciones de las partes que confían

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

#### 9.6.5. Obligaciones de otros participantes

335. No estipulado.

#### 9.7. RENUNCIA DE GARANTÍAS

336. No estipulado.



## 9.8. LIMITACIONES DE RESPONSABILIDAD

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

- No será responsable de la utilización de los *Certificados* emitidos bajo esta política cuando los representantes del *Suscriptor del Certificado* o *los miembros de Carrera Judicial* realicen actuaciones sin facultades o extralimitándose de las mismas.
- Las relaciones entre el órgano, organismo o entidad de la Administración Pública *Suscriptora del Certificado* y de los miembros de carrera judicial con la FNMT-RCM, se realizarán siempre a través de la *Oficina de Registro* y su responsable.

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

## 9.9. INDEMNIZACIONES

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

### 9.9.1. Indemnización de la CA

340. No estipulado.

### 9.9.2. Indemnización de los Suscriptores

341. No estipulado.

### 9.9.3. Indemnización de las partes que confían

342. No estipulado.

## 9.10. PERIODO DE VALIDEZ DE ESTE DOCUMENTO

### 9.10.1. Plazo

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

### 9.10.2. Terminación

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



**9.10.3. Efectos de la finalización**

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

**9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES**

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

**9.12. MODIFICACIONES DE ESTE DOCUMENTO**

**9.12.1. Procedimiento para las modificaciones**

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

**9.12.2. Periodo y mecanismo de notificación**

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

**9.12.3. Circunstancias bajo las cuales debe cambiarse un OID**

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

**9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS**

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

**9.14. NORMATIVA DE APLICACIÓN**

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

**9.15. CUMPLIMIENTO DE LA NORMATIVA APLICABLE**

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

**9.16. ESTIPULACIONES DIVERSAS**

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

**9.16.1. Acuerdo íntegro**

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

**9.16.2. Asignación**

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



**9.16.3. Severabilidad**

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

**9.16.4. Cumplimiento**

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

**9.16.5. Fuerza Mayor**

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

**9.17. OTRAS ESTIPULACIONES**

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