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

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

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

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

9.4. SOBRE EL SERVICIO DE SELLADO DE TIEMPO

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

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

10. CESE DE LA ACTIVIDAD DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN: TRANSFERENCIA DE LA PRESTACIÓN DEL SERVICIO.

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

167. En todo caso, la FNMT-RCM:

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

del servicio, por un periodo suficiente a los efectos que dictamine la legislación vigente.

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

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

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

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

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

11. DATOS DE CARÁCTER PERSONAL

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

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

- Tratar los datos siguiendo estrictamente las instrucciones de la FNMT-RCM;
- No aplicar o utilizar los datos personales obtenidos, para fines distintos a los que figuren en la presente Declaración General de Prácticas de Certificación;
- No comunicarlos a terceros, ni siquiera para su conservación;

- Guardar secreto profesional respecto de los mismos, aun después de finalizar sus relaciones con la FNMT-RCM y trasladar las obligaciones citadas en los párrafos anteriores al personal que dediquen al cumplimiento de la presente Declaración General de Prácticas de Certificación.
- Adoptar las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, de conformidad con lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.
- Destruir o devolver todos los datos de carácter personal objeto de tratamiento una vez finalice por cualquier causa la relación con la FNMT-RCM, salvo aquellos datos que la legislación obliga a conservarlos por un mínimo de quince (15) años.

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

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

174. Los datos personales del *Solicitante* una vez validados y su código de solicitud recogido en el paso de Presolicitud, se enviarán a la FNMT-RCM mediante comunicaciones seguras establecidas para tal fin entre la *Oficina de Registro* y la FNMT-RCM.

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

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

11.1.1. Información al Suscriptor

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

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

179. Los datos de carácter personal podrán ser comunicados sin consentimiento de los *Titulares* o *Suscriptores* del *Certificado* a otras Administraciones Públicas, sus organismos autónomos y demás entidades vinculadas o dependientes con el objetivo que éstas ejerzan sus respectivas competencias y siempre dentro del ámbito del artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social, y normativa de desarrollo. Todo ello, a los efectos de garantizar la prestación de los servicios de certificación y con la finalidad de comprobar la vigencia de los *Certificados* emitidos a los *Titulares,* permitiendo así la realización a través de medios electrónicos, informáticos y telemáticos de actuaciones en el ámbito de relaciones de derecho público.

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

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

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

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

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

11.1.2. Información a la Entidad usuaria

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

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

186. No obstante, y con carácter general, cualquier registro o utilización para otros fines distintos de los anteriores o no autorizados requiere del *Consentimiento* previo de los titulares de los datos así como de otras previsiones contempladas en la Ley. Su incumplimiento está sancionado en la *LOPD* con multas que pueden alcanzar los 600.000 euros por cada una de las infracciones cometidas y sin perjuicio de la incoación de acciones penales de acuerdo con el Capitulo I del Título X del Código Penal así como de reclamaciones privadas de los afectados.

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

11.1.3. Documento de seguridad LOPD

11.1.3.1. Objetivo y presentación del Documento de Seguridad LOPD

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

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

190. La presente Normativa de Seguridad tiene por objeto preservar los datos personales procesados dentro del *Prestador de Servicios de Certificación* de la FNMT-RCM, por lo que afectará a todos aquellos recursos (personal, máquinas, aplicativos, métodos) que estén implicados en el procesamiento de estos datos. Desde el Sistema de Información que desempeña las funciones de registro de los usuarios, donde se recaban los datos, hasta el almacenamiento y archivo de los mismos en sistemas de *Directorio Seguro*, sistemas identificación y/o autorización, sistemas de archivado y registro de eventos y cualquier otro

que pudiera existir interviniente en la prestación de servicios de certificación, incluyendo los interfaces y medios de comunicación entre los diferentes sistemas, ya sean redes telemáticas privadas o públicas.

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

192. La responsabilidad de todos los ficheros que contienen datos de carácter personal declarados por la FNMT-RCM corresponde a dicha entidad, ya que es la persona jurídica que decide sobre la finalidad, usos y contenido de los ficheros. No obstante, en lo que respecta al Fichero de "Usuarios de Sistemas EIT", el Director de Sistemas de Información de la FNMT-RCM es la persona facultada para decidir y autorizar sobre el uso y tratamiento de éste en representación de la FNMT-RCM.

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

11.1.3.2. Normas y estándares

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

Directivas Europeas

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

Legislación Española

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

11.1.3.3. Principios y normas de obligado cumplimiento

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

Funciones y obligaciones del personal

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

197. Existen una serie de funciones claramente diferenciadas en lo que respecta al personal implicado en el uso y tratamiento de los datos de carácter personal del Fichero de Usuarios de Sistemas EIT, como son: El *Responsable del Fichero*, el *Responsable de Seguridad*, el *Personal de Seguridad Informática*, *Administrador de la Aplicación*, *Usuarios de la Aplicación*, *Operador de backup*, *Auditor de Seguridad*. Estas funciones y, en su caso las personas que las asumen, se definen en el punto "*Documento de Seguridad LOPD*" del apartado "Definiciones" de la presente *Declaración General de Prácticas de Certificación*.

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

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

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

Subsistema de Gestión de Certificados

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

Subsistema de Oficina de Registro

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

Subsistema de Publicación

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

Procedimiento de notificación, gestión y respuesta ante las incidencias

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

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

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

206. Existe una base de datos de incidencias en la que se abren y se gestionan las incidencias. Cada persona puede realizar diferentes gestiones en función del rol que desempeñen. De modo resumido, cualquier persona perteneciente al PSC puede abrir una incidencia. Éstas son tratadas por personal del área correspondiente y una vez resuelta se cierra con la descripción de las acciones realizadas. En caso de que la incidencia conlleve modificaciones se abre una acción correctiva que es ejecutada por el personal al que compete la acción.

207. Los principales campos de una incidencia son:

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

Procedimientos de copias de seguridad y recuperación de datos

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

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

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

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

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

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

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

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

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

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

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

Control de acceso

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

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

- Control de acceso basado en perfiles: usando la identidad o el perfil del usuario del sistema, que solicita un acceso, junto con el modo de acceso solicitado.

- Se permitirá el acceso siempre que el usuario identificado solicite un modo de acceso que haya sido autorizado previamente; de lo contrario, se denegará.

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

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

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

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

Ficheros temporales

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

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

Gestión de soportes

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

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

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

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

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

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

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

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

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

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

Auditoría

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

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

Acceso Lógico

230. Existen varios tipos de acceso lógico al fichero:

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

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

- Cada usuario se identifica ante la aplicación con un nombre de usuario, que es único para cada persona.
- Todo usuario para autenticarse debe introducir una contraseña, que únicamente debe conocer el usuario que pretende autenticarse. Cada usuario es responsable de su contraseña y no debe compartirla con ningún otro.
- No se han creado grupos de personas que puedan acceder con un mismo usuario y contraseña, y tampoco existen usuarios genéricos. Las cuentas genéricas que se creen para pruebas o similares se eliminan inmediatamente después de realizar dichas pruebas.
- Cada usuario es libre de cambiar su contraseña si cree que esta puede estar comprometida, pero para ello debe haberla utilizado al menos durante un día. Sin perjuicio de lo anterior, el usuario tiene la obligación de no usar la misma contraseña durante un periodo superior a tres (3) años.
- Cuando un usuario se identifica y auténtica mas de tres veces de forma errónea el sistema bloquea la cuenta de dicho usuario.
- Existe un mecanismo de control: el Registro de Eventos, encargado de almacenar, entre otra información, todos los accesos a los distintos componentes de la infraestructura.

Acceso Físico

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

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

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

Pruebas con datos reales

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

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

11.1.3.4. Proceso de revisión

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

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

12. PROPIEDAD INTELECTUAL E INDUSTRIAL

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

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

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

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

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

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

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

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

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

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

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

248. Los servicios de validación de certificados realizados por la FNMT-RCM, principalmente mediante protocolo OCSP, no podrán ser objeto de reservicio, con o sin reventa, sin que exista valor añadido a los mismos. En caso de que se proporcione ese valor añadido para terceras partes, basándose en servicios de validación prestados por la FNMT-RCM, se debe solicitar a esta entidad la suscripción de un contrato OCSP para el tramo mayorista. Tal contrato se encuentra disponible en la página Web de la FNMT-RCM (Perfil del Contratante) y el solicitante deberá cumplir los requerimientos para su calificación como mayorista (prestación de servicios para terceros).

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

13. ORDEN DE PRELACIÓN

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

14. LEY APLICABLE, INTERPRETACIÓN Y JURISDICCIÓN COMPETENTE

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

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

competentes de la FNMT-RCM, cláusulas de arbitraje, de acuerdo con lo establecido en la Legislación aplicable.

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

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

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