

# **INFRAESTRUCTURA DE CLAVE PÚBLICA**

## **DNI ELECTRÓNICO**

**PROYECTO DE  
DECLARACIÓN DE  
PRÁCTICAS Y POLÍTICAS  
DE CERTIFICACIÓN**

**OID: 2.16.724.1.2.2.2.1.0.6**

## TABLA DE CONTENIDOS

|   | Pág.      |
|---|-----------|
| <b>1. INTRODUCCIÓN .....</b>  | <b>15</b> |
| <b>1.1 RESUMEN .....</b>  | <b>15</b> |
| <b>1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN.....</b>   | <b>17</b> |
| <b>1.3 ENTIDADES Y PERSONAS INTERVINIENTES.....</b>   | <b>17</b> |
| 1.3.1 Autoridad de Aprobación de Políticas .....  | 18        |
| 1.3.2 Autoridades de Certificación.....   | 18        |
| 1.3.3 Autoridades de Registro .....   | 21        |
| 1.3.4 Autoridad de Validación.....  | 21        |
| 1.3.5 Ciudadano.....  | 22        |
| 1.3.6 Usuario suscriptor (Ciudadano titular del DNle) .....   | 22        |
| 1.3.7 Terceros aceptantes .....   | 22        |
| <b>1.4 USO DE LOS CERTIFICADOS .....</b>  | <b>22</b> |
| 1.4.1 Usos apropiados de los certificados .....   | 22        |
| 1.4.2 Limitaciones y restricciones en el uso de los certificados .....  | 24        |
| 1.4.3 Fiabilidad de la firma electrónica a los largo del tiempo.....  | 25        |
| <b>1.5 ADMINISTRACIÓN DE LAS POLÍTICAS.....</b>   | <b>25</b> |
| 1.5.1 La Dirección General de la Policía como Órgano responsable del DNle .....                                 | 25        |
| 1.5.2 Persona de contacto .....   | 26        |
| 1.5.3 Determinación de la adecuación de la DPC de una AC externa a las Políticas de Certificación de DNle ..... | 26        |
| 1.5.4 Procedimientos de aprobación de esta DPC .....  | 26        |
| <b>1.6 DEFINICIONES Y ACRÓNIMOS .....</b>   | <b>26</b> |
| 1.6.1 Definiciones.....   | 26        |
| 1.6.2 Acrónimos.....  | 28        |

## TABLA DE CONTENIDOS

|   | Pág.      |
|---|-----------|
| <b>2. REPOSITARIOS Y PUBLICACIÓN DE INFORMACIÓN .....</b>   | <b>30</b> |
| <b>2.1 REPOSITARIOS .....</b>   | <b>30</b> |
| <b>2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN .....</b>  | <b>30</b> |
| <b>2.3 TEMPORALIDAD O FRECUENCIA DE PUBLICACIÓN .....</b>   | <b>31</b> |
| <b>2.4 CONTROLES DE ACCESO A LOS REPOSITARIOS .....</b>   | <b>31</b> |
| <b>3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS</b>                               | <b>32</b> |
| <b>3.1 NOMBRES .....</b>  | <b>32</b> |
| 3.1.1 Tipos de nombres.....   | 32        |
| 3.1.2 Necesidad de que los nombres sean significativos .....  | 32        |
| 3.1.3 Reglas para interpretar varios formatos de nombres.....   | 32        |
| 3.1.4 Unicidad de los nombres .....   | 33        |
| 3.1.5 Procedimientos de resolución de conflictos sobre nombres .....                                    | 33        |
| 3.1.6 Reconocimiento, autenticación y papel de las marcas registradas.....                              | 33        |
| <b>3.2 VALIDACIÓN DE LA IDENTIDAD INICIAL .....</b>   | <b>33</b> |
| 3.2.1 Medio de prueba de posesión de la clave privada .....   | 33        |
| 3.2.2 Autenticación de la identidad de una persona jurídica .....                                       | 34        |
| 3.2.3 Autenticación de la identidad de una persona física .....   | 34        |
| 3.2.4 Información no verificada sobre el solicitante .....  | 35        |
| 3.2.5 Comprobación de las facultades de representación .....  | 35        |
| 3.2.6 Criterios para operar con AC externas .....   | 35        |
| <b>3.3 IDENTIFICACIÓN Y AUTENTICACIÓN EN LAS PETICIONES DE RENOVACIÓN DE CLAVES Y CERTIFICADOS.....</b> | <b>35</b> |
| 3.3.1 Identificación y autenticación por una renovación de claves de rutina .....                       | 35        |

## TABLA DE CONTENIDOS

|  | Pág.      |
|--|-----------|
| 3.3.2 Identificación y autenticación para una renovación de claves tras una revocación ..... | 36        |
| <b>4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS .....</b>           | <b>36</b> |
| <b>4.1 SOLICITUD DE CERTIFICADOS .....</b>   | <b>36</b> |
| 4.1.1 Quién puede efectuar una solicitud .....   | 36        |
| 4.1.2 Registro de las solicitudes de certificados.....                                       | 37        |
| <b>4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS .....</b>                              | <b>38</b> |
| 4.2.1 Realización de las funciones de identificación y autenticación.                        | 38        |
| 4.2.2 Aprobación o denegación de las solicitudes de certificados .....                       | 38        |
| 4.2.3 Plazo para la tramitación de las solicitudes de certificados.....                      | 39        |
| <b>4.3 EMISIÓN DE CERTIFICADOS .....</b>   | <b>39</b> |
| 4.3.1 Actuaciones de la AC durante la emisión de los certificados ...                        | 39        |
| 4.3.2 Notificación al solicitante de la emisión por la AC del certificado                    | 40        |
| <b>4.4 ACEPTACIÓN DEL CERTIFICADO .....</b>  | <b>40</b> |
| 4.4.1 Forma en la que se acepta el certificado .....   | 40        |
| 4.4.2 Publicación del certificado por la AC .....  | 41        |
| 4.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades .....         | 41        |
| <b>4.5 PAR DE CLAVES Y USO DEL CERTIFICADO .....</b>   | <b>41</b> |
| 4.5.1 Uso de la clave privada y del certificado por el titular .....                         | 41        |
| 4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes .....            | 41        |
| <b>4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES.....</b>                              | <b>42</b> |
| 4.6.1 Circunstancias para la renovación de certificados sin cambio de claves.....            | 42        |

## TABLA DE CONTENIDOS

|  | Pág.      |
|--|-----------|
| <b>4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES .....</b>                                 | <b>42</b> |
| 4.7.1 Circunstancias para una renovación con cambio claves de un certificado .....               | 42        |
| 4.7.2 Quién puede pedir la renovación de un certificado.....                                     | 43        |
| 4.7.3 Tramitación de las peticiones de renovación con cambio de claves.....                      | 43        |
| 4.7.4 Notificación de la emisión de nuevos certificado al titular .....                          | 45        |
| 4.7.5 Forma de aceptación del certificado con nuevas claves .....                                | 45        |
| 4.7.6 Publicación del certificado con las nuevas claves por la AC ....                           | 45        |
| 4.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades .....             | 45        |
| <b>4.8 MODIFICACIÓN DE CERTIFICADOS .....</b>  | <b>45</b> |
| 4.8.1 Causas para la modificación de un certificado .....  | 45        |
| <b>4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS .....</b>   | <b>45</b> |
| 4.9.1 Causas para la revocación .....  | 46        |
| 4.9.2 Quién puede solicitar la revocación .....  | 47        |
| 4.9.3 Procedimiento de solicitud de revocación .....   | 47        |
| 4.9.4 Periodo de gracia de la solicitud de revocación .....                                      | 48        |
| 4.9.5 Plazo en el que la AC debe resolver la solicitud de revocación                             | 48        |
| 4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes .....           | 48        |
| 4.9.7 Frecuencia de emisión de CRLs.....   | 48        |
| 4.9.8 Tiempo máximo entre la generación y la publicación de las CRL4                             | 48        |
| 4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados ..... | 48        |
| 4.9.10 Requisitos de comprobación en-línea de revocación.....                                    | 49        |
| 4.9.11 Otras formas de divulgación de información de revocación                                  | 49        |

## TABLA DE CONTENIDOS

|   | Pág.      |
|---|-----------|
| disponibles .....   | 49        |
| 4.9.12 Requisitos especiales de renovación de claves comprometidas                    | 49        |
| 4.9.13 Circunstancias para la suspensión.....   | 49        |
| 4.9.14 Quién puede solicitar la suspensión.....                                       | 49        |
| 4.9.15 Procedimiento para la solicitud de suspensión .....                            | 49        |
| 4.9.16 Límites del periodo de suspensión.....   | 49        |
| <b>4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS.....</b>                  | <b>49</b> |
| 4.10.1 Características operativas .....   | 49        |
| 4.10.2 Disponibilidad del servicio.....   | 50        |
| 4.10.3 Características adicionales .....  | 50        |
| <b>4.11 FINALIZACIÓN DE LA SUSCRIPCION.....</b>                                       | <b>50</b> |
| <b>4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES .....</b>                                   | <b>50</b> |
| 4.12.1 Prácticas y políticas de custodia y recuperación de claves.....                | 50        |
| 4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión.....  | 50        |
| <b>5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES .....</b> | <b>51</b> |
| <b>5.1 CONTROLES FÍSICOS .....</b>  | <b>51</b> |
| 5.1.1 Ubicación física y construcción .....   | 51        |
| 5.1.2 Acceso físico .....   | 51        |
| 5.1.3 Alimentación eléctrica y aire acondicionado .....                               | 52        |
| 5.1.4 Exposición al agua.....   | 52        |
| 5.1.5 Protección y prevención de incendios .....                                      | 52        |
| 5.1.6 Sistema de almacenamiento .....   | 52        |
| 5.1.7 Eliminación de los soportes de información .....                                | 53        |

## TABLA DE CONTENIDOS

|   | Pág.      |
|---|-----------|
| 5.1.8 Copias de seguridad fuera de las instalaciones.....                                     | 53        |
| <b>5.2 CONTROLES DE PROCEDIMIENTO .....</b>   | <b>53</b> |
| 5.2.1 Roles responsables del control y gestión de la PKI.....                                 | 53        |
| 5.2.2 Número de personas requeridas por tarea .....   | 54        |
| 5.2.3 Identificación y autenticación para cada usuario .....                                  | 54        |
| 5.2.4 Roles que requieren segregación de funciones .....                                      | 54        |
| <b>5.3 CONTROLES DE PERSONAL .....</b>  | <b>55</b> |
| 5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales ..... | 55        |
| 5.3.2 Procedimientos de comprobación de antecedentes .....                                    | 55        |
| 5.3.3 Requerimientos de formación.....  | 55        |
| 5.3.4 Requerimientos y frecuencia de actualización de la formación                            | 55        |
| 5.3.5 Frecuencia y secuencia de rotación de tareas .....                                      | 56        |
| 5.3.6 Sanciones por actuaciones no autorizadas.....   | 56        |
| 5.3.7 Requisitos de contratación de terceros .....  | 56        |
| 5.3.8 Documentación proporcionada al personal .....   | 56        |
| <b>5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD .....</b>                                     | <b>56</b> |
| 5.4.1 Tipos de eventos registrados.....   | 56        |
| 5.4.2 Frecuencia de procesado de registros de auditoría.....                                  | 58        |
| 5.4.3 Periodo de conservación de los registros de auditoría .....                             | 58        |
| 5.4.4 Protección de los registros de auditoría.....   | 58        |
| 5.4.5 Procedimientos de respaldo de los registros de auditoría.....                           | 58        |
| 5.4.6 Sistema de recogida de información de auditoría .....                                   | 59        |
| 5.4.7 Notificación al sujeto causa del evento .....   | 59        |
| 5.4.8 Análisis de vulnerabilidades .....  | 59        |

## TABLA DE CONTENIDOS

|   | Pág.      |
|---|-----------|
| <b>5.5 ARCHIVO DE REGISTROS .....</b>   | <b>60</b> |
| 5.5.1 Tipo de eventos archivados.....   | 60        |
| 5.5.2 Periodo de conservación de registros.....   | 60        |
| 5.5.3 Protección del archivo .....  | 60        |
| 5.5.4 Procedimientos de copia de respaldo del archivo .....   | 60        |
| 5.5.5 Requerimientos para el sellado de tiempo de los registros .....   | 61        |
| 5.5.6 Sistema de archivo de información de auditoría .....  | 61        |
| 5.5.7 Procedimientos para obtener y verificar información archivada.....  | 61        |
| <b>5.6 CAMBIO DE CLAVES DE UNA AC .....</b>   | <b>61</b> |
| <b>5.7 RECUPERACIÓN EN CASOS DE VULNERACIÓN DE UNA CLAVE Y DE DESATRE NATURAL U OTRO TIPO DE CATÁSTROFE .....</b> | <b>62</b> |
| 5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades ...  | 62        |
| 5.7.2 Alteración de los recursos hardware, software y/o datos .....   | 62        |
| 5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una Autoridad .....                | 62        |
| 5.7.4 Instalación después de un desastre natural u otro tipo de catástrofe .....                                  | 63        |
| <b>5.8 CESE DE UNA AC O AR .....</b>  | <b>63</b> |
| 5.8.1 Autoridad de Certificación.....   | 63        |
| 5.8.2 Autoridad de Registro .....   | 64        |
| <b>6. CONTROLES DE SEGURIDAD TÉCNICA.....</b>   | <b>65</b> |
| <b>6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES .....</b>   | <b>65</b> |
| 6.1.1 Generación del par de claves .....  | 65        |
| 6.1.2 Entrega de la clave privada al titular .....  | 65        |
| 6.1.3 Entrega de la clave publica al emisor del certificado .....   | 65        |
| 6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes.....   | 65        |

## TABLA DE CONTENIDOS

|  | Pág.      |
|--|-----------|
| 6.1.5 Tamaño de las claves.....  | 66        |
| 6.1.6 Parámetros de generación de la clave pública y verificación de la calidad .....                  | 66        |
| 6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3) ...                                      | 66        |
| <b>6.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS.....</b> | <b>67</b> |
| 6.2.1 Estándares para los módulos criptográficos .....   | 67        |
| 6.2.2 Control multipersona (k de n) de la clave privada .....  | 67        |
| 6.2.3 Custodia de la clave privada .....   | 68        |
| 6.2.4 Copia de seguridad de la clave privada .....   | 69        |
| 6.2.5 Archivo de la clave privada .....  | 69        |
| 6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico .....                        | 69        |
| 6.2.7 Almacenamiento de la clave privada en un módulo criptográfico                                    | 66        |
| 6.2.8 Método de activación de la clave privada .....   | 70        |
| 6.2.9 Método de desactivación de la clave privada.....   | 70        |
| 6.2.10 Método de destrucción de la clave privada .....   | 70        |
| <b>6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES .....</b>  | <b>71</b> |
| 6.3.1 Archivo de la clave pública.....   | 71        |
| 6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves .....             | 71        |
| <b>6.4 DATOS DE ACTIVACIÓN.....</b>  | <b>72</b> |
| 6.4.1 Generación e instalación de los datos de activación .....  | 72        |
| 6.4.2 Protección de los datos de activación .....  | 72        |
| 6.4.3 Otros aspectos de los datos de activación .....  | 73        |
| <b>6.5 CONTROLES DE SEGURIDAD INFORMÁTICA .....</b>  | <b>73</b> |

## TABLA DE CONTENIDOS

|            | Pág.  |
|------------|---|
| 6.5.1      | Requerimientos técnicos de seguridad específicos .....73            |
| 6.5.2      | Evaluación de la seguridad informática .....74                      |
| <b>6.6</b> | <b>CONTROLES DE SEGURIDAD DEL CICLO DE VIDA ..... 74</b>            |
| 6.6.1      | Controles de desarrollo de sistemas .....74                         |
| 6.6.2      | Controles de gestión de seguridad .....74                           |
| 6.6.3      | Controles de seguridad del ciclo de vida .....75                    |
| <b>6.7</b> | <b>CONTROLES DE SEGURIDAD DE LA RED ..... 75</b>                    |
| <b>6.8</b> | <b>FUENTES DE TIEMPO ..... 75</b>                                   |
| <b>7.</b>  | <b>PERFILES DE LOS CERTIFICADOS, CRL Y OCSP ..... 76</b>            |
| <b>7.1</b> | <b>PERFIL DE CERTIFICADO ..... 76</b>                               |
| 7.1.1      | Número de versión .....76   |
| 7.1.2      | Extensiones del certificado.....76                                  |
| 7.1.3      | Identificadores de objeto (OID) de los algoritmos .....84           |
| 7.1.4      | Formatos de nombres .....84   |
| 7.1.5      | Restricciones de los nombres .....84                                |
| 7.1.6      | Identificador de objeto (OID) de la Política de Certificación....84 |
| 7.1.7      | Uso de la extensión "PolicyConstraints" .....85                     |
| 7.1.8      | Sintaxis y semántica de los "PolicyQualifier" .....85               |
| 7.1.9      | Tratamiento semántico para la extensión "Certificate Policy" .85    |
| <b>7.2</b> | <b>PERFIL DE CRL..... 86</b>  |
| 7.2.1      | Número de versión .....86   |
| 7.2.2      | CRL y extensiones .....86   |
| <b>7.3</b> | <b>PERFIL DE OCSP ..... 86</b>                                      |
| 7.3.1      | Perfil del certificado OCSP responder .....86                       |

## TABLA DE CONTENIDOS

|  | Pág.      |
|--|-----------|
| 7.3.2 Número de versión .....  | 86        |
| 7.3.3 Formatos de nombres .....  | 87        |
| 7.3.4 Identificador de objeto (OID) de la Política de Certificación....          | 87        |
| 7.3.5 Extensiones y Campos del certificado .....                                 | 88        |
| 7.3.6 formato de las peticiones OCSP .....                                       | 90        |
| 7.3.7 formato de las respuestas .....  | 90        |
| 7.3.8 Fechado respuestas omsp.....   | 91        |
| <b>8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES .....</b>                     | <b>91</b> |
| 8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA<br>AUTORIDAD .....    | 91        |
| 8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....                                | 91        |
| 8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA .....                      | 92        |
| 8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES .....                                   | 92        |
| 8.5 ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE<br>DEFICIENCIAS ..... | 92        |
| 8.6 COMUNICACIÓN DE RESULTADOS .....   | 92        |
| <b>9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD .....</b>                          | <b>93</b> |
| 9.1 TARIFAS.....   | 93        |
| 9.1.1 Tarifas de emisión de certificado o renovación .....                       | 93        |
| 9.1.2 Tarifas de acceso a los certificados .....                                 | 93        |
| 9.1.3 Tarifas de acceso a la información de estado o revocación.....             | 93        |
| 9.1.4 Tarifas de otros servicios tales como información de políticas             | 93        |
| 9.1.5 Política de reembolso .....  | 94        |
| <b>9.2 RESPONSABILIDADES ECONÓMICAS .....</b>                                    | <b>94</b> |

## TABLA DE CONTENIDOS

|   | Pág.       |
|---|------------|
| <b>9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN .....</b>                             | <b>94</b>  |
| 9.3.1  Ámbito de la información confidencial.....                               | 94         |
| 9.3.2  Información no confidencial .....  | 95         |
| 9.3.3  Deber de secreto profesional.....  | 95         |
| <b>9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL.....</b>                           | <b>95</b>  |
| 9.4.1  Política de protección de datos de carácter personal .....               | 95         |
| 9.4.2  Información tratada como privada .....                                   | 95         |
| 9.4.3  Información no calificada como privada .....                             | 96         |
| 9.4.4  Responsabilidad de la protección de los datos de carácter personal ..... | 96         |
| 9.4.5  Comunicación y consentimiento para usar datos de carácter personal ..... | 97         |
| 9.4.6  Revelación en el marco de un proceso judicial .....                      | 97         |
| 9.4.7  Otras circunstancias de publicación de información .....                 | 97         |
| <b>9.5 DERECHOS DE PROPIEDAD INTELECTUAL .....</b>                              | <b>97</b>  |
| <b>9.6 OBLIGACIONES .....</b>   | <b>97</b>  |
| 9.6.1  Obligaciones de la AC .....  | 97         |
| 9.6.2  Obligaciones de la AR .....  | 99         |
| 9.6.3  Obligaciones de los ciudadanos titulares de los certificados ...         | 99         |
| 9.6.4  Obligaciones de los terceros aceptantes.....                             | 100        |
| 9.6.5  Obligaciones de otros participantes.....                                 | 101        |
| <b>9.7 LIMITACIONES DE RESPONSABILIDAD.....</b>                                 | <b>101</b> |
| <b>9.8 RESPONSABILIDADES.....</b>   | <b>101</b> |
| 9.8.1  Limitaciones de responsabilidades .....                                  | 101        |
| 9.8.2  Responsabilidades de la Autoridad de Certificación .....                 | 101        |

## TABLA DE CONTENIDOS

|  | Pág.       |
|--|------------|
| 9.8.3 Responsabilidades de la Autoridad de Registro .....                                | 102        |
| 9.8.4 Responsabilidades del ciudadano .....  | 103        |
| 9.8.5 Delimitación de responsabilidades.....   | 103        |
| 9.8.6 Alcance de la cobertura .....  | 103        |
| 9.8.7 Cobertura de seguro u otras garantías para los terceros<br>aceptantes .....        | 104        |
| <b>9.9 LIMITACIONES DE PÉRDIDAS .....</b>  | <b>104</b> |
| <b>9.10 PERIODO DE VALIDEZ.....</b>  | <b>104</b> |
| 9.10.1 Plazo .....   | 104        |
| 9.10.2 Sustitución y derogación de la DPC .....  | 104        |
| 9.10.3 Efectos de la finalización .....  | 105        |
| <b>9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS<br/>PARTICIPANTES .....</b> | <b>105</b> |
| <b>9.12 PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES .....</b>                      | <b>105</b> |
| 9.12.1 Procedimiento para los cambios.....   | 105        |
| 9.12.2 Periodo y procedimiento de notificación .....                                     | 105        |
| 9.12.3 Circunstancias en las que el OID debe ser cambiado.....                           | 105        |
| <b>9.13 RECLAMACIONES Y JURISDICCIÓN .....</b>   | <b>106</b> |
| <b>9.14 NORMATIVA APLICABLE .....</b>  | <b>106</b> |
| <b>9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE.....</b>                                  | <b>106</b> |
| <b>9.16 ESTIPULACIONES DIVERSAS .....</b>  | <b>107</b> |
| 9.16.1 Cláusula de aceptación completa .....   | 107        |
| 9.16.2 Independencia .....   | 107        |
| 9.16.3 Resolución por la vía judicial .....  | 107        |
| <b>9.17 OTRAS ESTIPULACIONES .....</b>   | <b>107</b> |

## TABLA DE CONTENIDOS

|  | Pág.       |
|--|------------|
| <b>10. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.....</b>       | <b>108</b> |
| <b>10.1 RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS.....</b>       | <b>108</b> |
| <b>10.2 CREACIÓN DEL FICHERO E INSCRIPCIÓN REGISTRAL .....</b> | <b>108</b> |
| <b>10.3 DOCUMENTO DE SEGURIDAD LOPD.....</b>                   | <b>109</b> |
| 10.3.1 Aspectos cubiertos .....                                | 109        |
| 10.3.2 Funciones y obligaciones del personal .....             | 110        |
| 10.3.3 Estructura de datos de carácter personal .....          | 110        |
| 10.3.4 Nivel de seguridad.....                                 | 111        |
| 10.3.5 Sistemas de información .....                           | 111        |
| 10.3.6 Relación de usuarios.....                               | 111        |
| 10.3.7 Notificación y gestión de incidencias.....              | 111        |
| 10.3.8 Copias de respaldo y recuperación .....                 | 111        |
| 10.3.9 Control de accesos .....                                | 112        |
| 10.3.10 Ficheros temporales .....                              | 112        |
| 10.3.11 Gestión de soportes .....                              | 112        |
| 10.3.12 Utilización de datos reales en pruebas.....            | 113        |
| <b>ÚLTIMOS CAMBIOS.....</b>                                    | <b>114</b> |

## 1. INTRODUCCIÓN

### 1.1 RESUMEN

La **Ley 59/2003**, de **19 de diciembre**, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.

Este nuevo mecanismo de identificación basado en el actual Documento Nacional de Identidad, cuya expedición se regula por el **Real Decreto 1553/2005**, de **23 de diciembre**, permitirá al ciudadano establecer sus relaciones de confianza con terceros a través de las nuevas tecnologías, tal y como lo lleva haciendo durante más de 50 años con el actual Documento.

Para ello el Órgano encargado de la expedición y gestión del DNI – La Dirección General de la Policía tal y como recoge el RD - implantará una Infraestructura de Clave Pública, que dotará al nuevo DNI de los certificados electrónicos necesarios para cumplir adecuadamente con los objetivos anteriores

El presente documento recoge la Declaración de Prácticas y Políticas de Certificación (DPC) que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública de los Certificados de identidad pública y firma electrónica del Documento Nacional de Identidad (desde ahora DNIE). La presente DPC recoge también las Políticas de Certificación que la Dirección General de la Policía (Ministerio del Interior) emplea en la gestión de certificados.

Esta DPC se aplica a todos los intervinientes relacionados con la jerarquía del DNI Electrónico, incluyendo Autoridades de Certificación (AC), Autoridades de Registro, Ciudadanos y Terceros Aceptantes, entre otros.

La presente DPC se ha estructurado conforme a lo dispuesto por el grupo de trabajo PKIX del IETF (Internet Engineering Task Force), en su documento de referencia RFC 3647 (aprobado en Noviembre de 2003) *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"*. A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC 3647. Cuando no se haya previsto nada en alguna sección aparecerá la frase "No estipulado". Adicionalmente a los epígrafes establecidos en la RFC 3647, se ha incluido un capítulo adicional dedicado a la protección de datos de carácter personal para dar cumplimiento a la normativa española en la materia.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta a los estándares europeos, entre los que cabe destacar los siguientes:

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

Esta DPC recoge la política de servicios, así como la declaración del nivel de garantía ofrecido, mediante la descripción de las medidas técnicas y organizativas establecidas para garantizar el nivel de seguridad de la PKI.

La DPC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía de la relación entre DNIE y sus usuarios. En consecuencia, todas las partes involucradas tienen la obligación de conocer la DPC y ajustar su actividad a lo dispuesto en la misma.

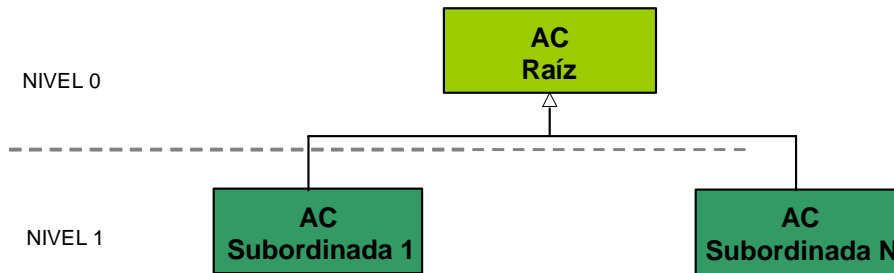
Los Certificados de Identidad Pública serán emitidos como **Certificados Electrónicos Reconocidos** cumpliendo los requisitos del anexo I de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, así como lo dispuesto a tal efecto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. El prestador de servicios de certificación, Dirección General de la Policía (Ministerio del Interior), cumplirá los requisitos expresados en el anexo II de la directiva indicada anteriormente, y desarrollado en Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Asimismo, los certificados cumplen los estándares en materia de certificados reconocidos, en concreto:

- ETSI TS 101 862: Qualified Certificate Profile.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

De acuerdo con la legislación señalada, se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Esta DPC asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

La arquitectura general, a nivel jerárquico, de la PKI del DNI Electrónico es la siguiente:



- Un primer nivel en el que se ubica la AC raíz que representa el punto de confianza de todo el sistema y que permitirá, tal y como recoge el artículo 15 de la Ley de Firma electrónica, que todas las personas físicas o jurídicas, públicas o privadas, reconozcan la eficacia del Documento Nacional de Identidad electrónico para acreditar la identidad.
- Un segundo nivel, constituido por las AC subordinadas de la AC Raíz que emitirán los certificados de identidad y firma del nuevo DNI.

## 1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

|                                |   |
|--------------------------------|---|
| <b>Nombre del documento</b>    | Declaración de Prácticas y Políticas de Certificación (DPC)                     |
| <b>Versión del documento</b>   | 1.0   |
| <b>Estado del documento</b>    | Vigente   |
| <b>Fecha de emisión</b>        | 02/02/2006  |
| <b>Fecha de caducidad</b>      | No aplicable  |
| <b>OID (Object Identifier)</b> | 2.16.724.1.2.2.2.1.0.6  |
| <b>Ubicación de la DPC</b>     | <a href="http://www.dnielectronico.es/dpc">http://www.dnielectronico.es/dpc</a> |

## 1.3 ENTIDADES Y PERSONAS INTERVINIENTES

Las entidades y personas intervinientes son:

- La Dirección General de la Policía como Órgano competente de la expedición y gestión del DNIe.
- La Autoridad de Aprobación de Políticas.
- Las Autoridades de Certificación.
- Las Autoridades de Registro.
- Las Autoridades de Validación.
- Los ciudadanos como solicitantes del DNIe.

- Los ciudadanos titulares del DNIE.
- Los Terceros Aceptantes de los certificados emitidos por DNIE incluyendo Prestadores de Servicios telemáticos basados en la utilización del DNIE.

### 1.3.1 Autoridad de Aprobación de Políticas

La Autoridad de Aprobación de Políticas (AAP) creada dentro de la Dirección General de la Policía como comité ejecutivo de la Infraestructura de Clave Pública (PKI), bajo la autoridad del Ministro del Interior tiene atribuida la función de elaboración y propuesta de aprobación de la presente DPC, así como de sus modificaciones.

La presente DPC será aprobada mediante Orden Ministerial que se publicará en el Boletín Oficial del Estado.

Asimismo, la AAP es la responsable, en caso de que se tuviese que evaluar la posibilidad de que una AC externa interactúe con la PKI del DNIE, de determinar la adecuación de la DPC de dicha AC a esta DPC y de regular de la Prestación del Servicio de Validación por parte de terceros

La AAP es también la encargada de analizar los informes de las auditorías, totales o parciales, que se hagan de DNIE, así como de determinar, en caso necesario, las acciones correctoras a ejecutar.

### 1.3.2 Autoridades de Certificación

La Dirección General de la Policía (Ministerio del Interior) actúa como Autoridad de Certificación (AC), relacionando dos pares de claves con un ciudadano concreto a través de la emisión de sendos Certificados de conformidad con los términos de esta DPC.

Las Autoridades de Certificación que componen la PKI del DNIE son:

- **"AC Raíz"**: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. Sus datos más relevantes son:

|  |   |
|--|---|
| <b>Nombre Distintivo</b>                           | CN= AC RAIZ DNIE, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES                            |
| <b>Certificado pkcs1-sha1WithRSAEncryption (*)</b> |   |
| <b>Número de serie</b>                             | 00 d2 85 70 fd ae a7 d6 5f 11 84 15 c6 31 b5 cb   |
| <b>Periodo de validez</b>                          | Desde jueves, 16 de febrero de 2006 11:37:25<br>hasta viernes, 08 de febrero de 2036 23:59:59 |
| <b>Huella Digital (SHA-1)</b>                      | b3 8f ec ec 0b 14 8a a6 86 c3 d0 0f 01 ec c8 84 8e 80 85 eb                                   |
| <b>Huella Digital (MD5)</b>                        | 15 5e f5 11 7a a2 c1 15 0e 92 7e 66 fe 3b 84 c3   |
| <b>Certificado pkcs1-sha256WithRSAEncryption</b>   |   |
| <b>Número de serie</b>                             | 00 c5 26 c9 6e 10 94 ed 43 4f f7 b5 fb 67 9f 94   |
| <b>Periodo de validez</b>                          | Desde jueves, 16 de febrero de 2006 11:37:25<br>hasta viernes, 08 de febrero de 2036 23:59:59 |

---

**Huella Digital (SHA-1)** 22 29 f0 56 d3 4d 1c b6 3e 98 6f 26 b2 d0 8a b9 4f f0 8e 4d

---

**Huella Digital (MD5)** 0b 7d ca a8 ba c2 29 1d cf c7 11 36 38 c7 e7 ed

---

(\*) El certificado con algoritmo de firma **pkcs1-sha1WithRSAEncryption** se publica por razones de interoperabilidad, para facilitar a aquellos sistemas y aplicaciones que no soporten **pkcs1-sha256WithRSAEncryption**, construir la cadena de confianza en los procesos de validación de certificados y firma. Estos sistemas y aplicaciones tienen un plazo máximo de dos años para realizar las adaptaciones que sean necesarias para soportar dicho algoritmo. A partir de esa fecha la DPC se revisará para indicar de forma expresa que dicho certificado deja de tener efecto.

- **"AC Subordinadas"**: Autoridades de Certificación subordinadas de "AC Raíz". Su función es la emisión de certificados para los titulares de DNIE.

En el momento de publicación de la presente DPC, el dominio de certificación del DNIE consta de las siguientes AC subordinadas:

#### Autoridad de Certificación Subordinada 001

---

**Nombre Distintivo** CN= AC DNIE 001, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES

---

**Certificado pkcs1-sha1WithRSAEncryption (\*)**

---

**Número de serie** 64 20 66 c9 99 7b ae e1 44 02 da 6e a4 22 d6 49

---

**Periodo de validez** Desde lunes, 27 de febrero de 2006 11:54:38  
hasta viernes, 26 de febrero de 2021 23:59:59

---

**Estado** Operativa

---

**Huella Digital (SHA-1)** a3 4d 2c c5 32 45 80 a1 76 61 84 c7 a2 17 3f d0 f8 90 ec d0

---

**Huella Digital (MD5)** e6 94 20 22 b2 c1 0c 58 42 9f 42 4b 29 a7 66 df

---

**Certificado pkcs1-sha256WithRSAEncryption**

---

**Número de serie** 4c 2e fa 0f 77 11 2c 07 44 02 da 18 af b9 fe 7e

---

**Periodo de validez** Desde lunes, 27 de febrero de 2006 11:53:12  
Hasta viernes, 26 de febrero de 2021 23:59:59

---

**Estado** Operativa

---

**Huella Digital (SHA-1)** 41 cf 9e c0 73 3d 58 e4 39 97 a6 c6 5d f7 97 c3 ee 99 40 7b

---

**Huella Digital (MD5)** 7f 7b 17 27 2d e9 04 f2 8c 90 ac c5 98 af e7 0b

---

(\*) El certificado con algoritmo de firma **pkcs1-sha1WithRSAEncryption** se publica por razones de interoperabilidad, para facilitar a aquellos sistemas y aplicaciones que no soporten **pkcs1-sha256WithRSAEncryption**, construir la cadena de confianza en los procesos de validación de certificados y firma. Estos sistemas y aplicaciones tienen un plazo máximo de dos años para realizar las adaptaciones que sean necesarias para soportar dicho algoritmo. A partir de esa fecha la DPC se revisará para indicar de forma expresa que dicho certificado deja de tener efecto.

#### Autoridad de Certificación Subordinada 002

---

**Nombre Distintivo** CN= AC DNIE 002, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES

---

**Certificado pkcs1-sha1WithRSAEncryption (\*)**

|   |  |
|---|--|
| <b>Número de serie</b>                            | 38 34 6a ba 65 6b 04 b9 44 05 7f 34 34 7b e9 ae  |
| <b>Periodo de validez</b>                         | Desde miércoles, 01 de marzo de 2006 12:02:12<br>Hasta viernes, 26 de febrero de 2021 23:59:59 |
| <b>Estado</b>                                     | Operativa  |
| <b>Huella Digital (SHA-1)</b>                     | 38 37 90 17 0f 95 59 59 85 7b a7 06 40 f9 e0 06 8f 4b 14 08                                    |
| <b>Huella Digital (MD5)</b>                       | 4c 46 c2 56 39 14 25 25 01 dc 89 ab bc 9f dc 8f  |
| <b>Certificado pkcs1- sha256WithRSAEncryption</b> |  |
| <b>Número de serie</b>                            | 3e 02 bf 5b de 8e 3d 16 44 05 7e fa 56 4c 42 75  |
| <b>Periodo de validez</b>                         | Desde miércoles, 01 de marzo de 2006 12:01:14<br>Hasta viernes, 26 de febrero de 2021 23:59:59 |
| <b>Estado</b>                                     | Operativa  |
| <b>Huella Digital (SHA-1)</b>                     | 50 2b d0 07 8e 6d a2 35 c4 5f 52 1c 63 ef 54 9d f0 19 8f dd                                    |
| <b>Huella Digital (MD5)</b>                       | 5b 6a a3 c5 7a 68 9a eb 7d 29 70 1e 91 9c 4f 96  |

(\*) El certificado con algoritmo de firma **pkcs1-sha1WithRSAEncryption** se publica por razones de interoperabilidad, para facilitar a aquellos sistemas y aplicaciones que no soporten **pkcs1-sha256WithRSAEncryption**, construir la cadena de confianza en los procesos de validación de certificados y firma. Estos sistemas y aplicaciones tienen un plazo máximo de dos años para realizar las adaptaciones que sean necesarias para soportar dicho algoritmo. A partir de esa fecha la DPC se revisará para indicar de forma expresa que dicho certificado deja de tener efecto.

### Autoridad de Certificación Subordinada 003

|  |  |
|--|--|
| <b>Nombre Distintivo</b>                           | CN= AC DNIE 003, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES                              |
| <b>Certificado pkcs1-sha1WithRSAEncryption (*)</b> |  |
| <b>Número de serie</b>                             | 7c 49 0f ed 70 d1 e2 8b 44 05 7f 6e 8d 12 48 a3  |
| <b>Periodo de validez</b>                          | Desde miércoles, 01 de marzo de 2006 12:03:10<br>Hasta viernes, 26 de febrero de 2021 23:59:59 |
| <b>Estado</b>                                      | Operativa  |
| <b>Huella Digital (SHA-1)</b>                      | bb 85 a3 25 68 cd 68 40 53 03 83 10 32 12 76 f3 db c6 cf 97                                    |
| <b>Huella Digital (MD5)</b>                        | 5b514c7fe3c40758451d0ad896db74ca   |
| <b>Certificado pkcs1- sha256WithRSAEncryption</b>  |  |
| <b>Número de serie</b>                             | 08 f7 7b 06 6f b6 1b cd 44 05 7f 51 2e 0a db a8  |
| <b>Periodo de validez</b>                          | Desde miércoles, 01 de marzo de 2006 12:02:41<br>Hasta viernes, 26 de febrero de 2021 23:59:59 |
| <b>Estado</b>                                      | Operativa  |
| <b>Huella Digital (SHA-1)</b>                      | fb c0 71 d0 a4 81 11 bd df 77 76 d0 9e 42 bc 53 4e 24 48 70                                    |
| <b>Huella Digital (MD5)</b>                        | 67 a1 0e 56 91 c8 c5 8b e5 ba 91 8c ce 90 e8 7e  |

(\*) El certificado con algoritmo de firma **pkcs1-sha1WithRSAEncryption** se publica por razones de interoperabilidad, para facilitar a aquellos sistemas y aplicaciones que no soporten **pkcs1-sha256WithRSAEncryption**, construir la cadena de confianza en los procesos de validación de certificados y firma. Estos sistemas y aplicaciones tienen un plazo máximo de dos años para realizar las adaptaciones que sean necesarias para soportar dicho algoritmo. A partir de esa fecha la DPC se revisará para indicar de forma expresa que dicho certificado deja de tener efecto.

La incorporación de una nueva AC al dominio o el cese de operación de la misma serán causa de modificación de la presente DPC y de notificación a través de los mecanismos habilitados a tal efecto.

### 1.3.3 Autoridades de Registro

La Autoridad de Registro está constituida por todas las oficinas de expedición del Documento Nacional de Identidad, y tienen por misión realizar las funciones de asistencia a la Autoridad de Certificación en los procedimientos y trámites relacionados con los ciudadanos para su identificación, registro y autenticación y de esta forma garantizar la asignación de las claves al solicitante. La situación geográfica serán las Oficinas de Documentación de la Dirección General de la Policía y las instalaciones habilitadas para los equipos móviles, en aquellos lugares donde no existe Comisaría de Policía, así como otros lugares que a tal efecto determine el Órgano encargado de la expedición y gestión del DNle.

### 1.3.4 Autoridad de Validación

La(s) Autoridad(es) de Validación (AV) tienen como función la comprobación del estado de los certificados emitidos por DNle, mediante el protocolo *Online Certificate Status Protocol* (OCSP), que determina el estado actual de un certificado electrónico a solicitud de un Tercero Aceptante sin requerir el acceso a listas de certificados revocados por éstas.

Este servicio de consulta debe prestarse tal y como establece la Ley 59/2003, de firma electrónica, en su artículo 18 apartado d: garantizando *“la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.”*

El escenario inicial de segmentación de Autoridades de Validación (que cumple con los objetivos de universalidad y redundancia) es el siguiente:

- **Ministerio de Administraciones Públicas**, que prestaría los servicios de validación al conjunto de las Administraciones Públicas.
- **Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda**, que prestaría sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.

Los convenios que regulen las relaciones entre el PSC (DGP) y las Autoridades de Validación quedan fuera del alcance de este documento. No obstante a las Entidades que presten el servicio de validación les será de aplicación lo establecido en la legislación vigente para los Prestadores de Servicios de Certificación.

### 1.3.5 Ciudadano

A los efectos de esta DPC, se entiende como ciudadano a toda persona física con nacionalidad española que en nombre propio, y previa identificación, solicita la expedición o renovación de un Documento Nacional de Identidad ante un funcionario de la Dirección General de la Policía habilitado para esta práctica.

### 1.3.6 Usuario suscriptor (Ciudadano titular del DNI e)

Se entiende por usuario de los certificados al ciudadano español, mayor de edad y con plena capacidad de obrar, que voluntariamente confía y hace uso de los certificados contenidos en su Documento Nacional de Identidad y emitidos por la Dirección General de la Policía (Ministerio del Interior), de los cuales es titular.

Cuando un usuario decida voluntariamente confiar y hacer uso de alguno de sus certificados le será de aplicación la presente DPC.

### 1.3.7 Terceros aceptantes

Los Terceros Aceptantes son las personas o entidades diferentes del titular que deciden aceptar y confiar en un certificado emitido por DNIE. Tal y como recoge la Ley de Firma electrónica: *“Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.”*

Se entiende como prestador de servicios telemáticos a toda persona física o jurídica que ofrece al ciudadano la posibilidad de realizar transacciones telemáticas utilizando el DNIE.

## 1.4 USO DE LOS CERTIFICADOS

### 1.4.1 Usos apropiados de los certificados

Los Certificados de Identidad Pública, emitidos por la Dirección General de la Policía (Ministerio del Interior) tendrán como finalidad:

- **Certificado de Autenticación:** Garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios telemáticos no tendrán garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de

autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio telemáticos).

Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

- **Certificado de Firma:** El propósito de este certificado es permitir al ciudadano firmar trámites o documentos. Este certificado (certificado cualificado según ETSI, la RFC3739 y la Directiva Europea 99/93/EC. y reconocido según la ley de Firma Electrónica) permite sustituir la firma manuscrita por la electrónica en las relaciones del ciudadano con terceros (LFE 59/2003 artº 3.4 y 15.2).

Los certificados de firma son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículo 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Son certificados reconocidos que funcionan como dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3, de la Ley 59/2003, de 19 de diciembre. Por este motivo, garantizan la identidad del ciudadano poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha estado generada utilizando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita para efecto legal, sin necesidad de cumplir ningún otro requerimiento adicional.

Por lo anteriormente descrito, este certificado no deberá ser empleado para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio telemáticos).

El uso conjunto de ambos certificados proporciona las siguientes garantías:

- Autenticidad de origen

El Ciudadano podrá, a través de su **Certificado de Autenticación**, acreditar su identidad frente a cualquiera, demostrando la posesión y el acceso a la clave privada asociada a la pública que se incluye en el certificado que acredita su identidad. Ambos clave privada y certificado, se encuentran almacenados en el Documento Nacional de Identidad, el cual dispone de un procesador con capacidades criptográficas. Esto permite garantizar que la clave privada del ciudadano (punto en el que se basa la credibilidad de su identidad) no abandona en ningún momento el soporte físico del Documento Nacional de Identidad. De este modo el ciudadano, en el momento de acreditar electrónicamente su identidad, deberá estar en posesión de su DNI y de la clave personal de acceso (PIN) a la clave privada del certificado.

- No repudio de origen

Asegura que el documento proviene del ciudadano de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del **Certificado de Firma**. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando cualquiera de los Prestadores de Servicios de Validación del DNIe. De esta forma garantiza que el documento proviene de un determinado ciudadano.

Dado que el DNIe es un dispositivo seguro de creación de firma y que las claves de firma permanecen desde el momento de su creación bajo el control del ciudadano titular, se garantiza el compromiso del mismo con la firma realizada (garantía de “no repudio”).

- Integridad

Con el empleo del **Certificado de Firma**, se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de su resumen.

#### **1.4.2 Limitaciones y restricciones en el uso de los certificados**

Los certificados deben emplearse únicamente de acuerdo con la legislación que le sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia de criptografía existentes en cada momento.

Los certificados emitidos por la Dirección General de la Policía (Ministerio del Interior) solamente podrán emplearse para autenticación (acreditación de identidad) y para firmar electrónicamente (no repudio y compromiso con lo firmado).

El perfil de los certificados no contempla el uso de dichos certificados y sus claves asociadas para cifrar ningún tipo de información

Los certificados no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

Tal y como se recoge en el apartado anterior el certificado de autenticación no deberá emplearse para la firma de trámites y documentos en los que se precisa dejar constancia del compromiso del firmante con el contenido firmado. Igualmente el certificado de firma no deberá ser empleado para firmar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio telemáticos).

Los servicios de certificación que ofrece DNIe, no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como las relativas al funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otra donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

El DNIe es un dispositivo seguro de creación de firma y como tal, garantiza que las claves permanecen desde el momento de su creación bajo el control del ciudadano

titular del DNIE y que no es posible su exportación y uso desde cualquier otro dispositivo. El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de su tarjeta así como de los mecanismos de activación de las claves privadas, evitando su pérdida, divulgación, modificación o uso no autorizado.

### 1.4.3 Fiabilidad de la firma electrónica a los largo del tiempo

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, esta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que si queremos tener una firma que pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

La generación de una firma longeva debe incluir los siguientes elementos:

**Sello de tiempo:** Se ha de incluir en la firma un sello de tiempo emitido por una Tercera Parte de Confianza, TSA (Autoridad de Sellado de Tiempo). El sello de tiempo asegura que tanto los datos originales del documento como la información del estado de los certificados, se generaron antes de una determinada fecha. El formato del sello de tiempo debe seguir el estándar definido en la RFC3161.

**Información de revocación:** La firma ha de incluir un elemento que asegura que el certificado de firma es válido. Este elemento será generado una Tercera Parte de Confianza, en este caso por una de las Autoridades de Validación del DNI.

Es necesario que con posterioridad las firmas puedan renovarse (refirmado) y actualizar los elementos de confianza (sellos de tiempo) para dotar a las firmas electrónicas de validez a lo largo del tiempo, logrando garantizar su fiabilidad.

## 1.5 ADMINISTRACIÓN DE LAS POLÍTICAS

### 1.5.1 La Dirección General de la Policía como Órgano responsable del DNIE

Esta DPC es propiedad de la Dirección General de la Policía (Ministerio del Interior):

|                         |  |            |              |
|-------------------------|--|------------|--------------|
| <b>Nombre</b>           | Dirección General de la Policía (Ministerio del Interior)                          |            |              |
| <b>Dirección e-mail</b> | <a href="mailto:certificados@dnielectronico.es">certificados@dnielectronico.es</a> |            |              |
| <b>Dirección</b>        | C/Miguel Ángel 5 MADRID (España)   |            |              |
| <b>Teléfono</b>         | +34913223400   | <b>Fax</b> | +34913085774 |

### 1.5.2 Persona de contacto

Esta DPC está administrada por la Autoridad de Aprobación de Políticas (AAP) del DNI Electrónico.

|                         |  |            |              |
|-------------------------|--|------------|--------------|
| <b>Nombre</b>           | Grupo de trabajo del Certificado de Identidad Pública                              |            |              |
| <b>Dirección e-mail</b> | <a href="mailto:certificados@dnielectrónico.es">certificados@dnielectrónico.es</a> |            |              |
| <b>Dirección</b>        | C/Miguel Ángel 5 MADRID (España)   |            |              |
| <b>Teléfono</b>         | +34913223400   | <b>Fax</b> | +34913085774 |

### 1.5.3 Determinación de la adecuación de la DPC de una AC externa a las Políticas de Certificación de DNIe

En el caso de que se tuviese que evaluar la posibilidad de que una AC externa interactúe con la PKI del DNIe estableciendo relaciones de confianza, la Autoridad de Aprobación de Políticas (AAP) de DNIe es la responsable de determinar la adecuación de la DPC de la AC externa a la Política de Certificación afectada.

### 1.5.4 Procedimientos de aprobación de esta DPC

La Autoridad de Aprobación de Políticas (AAP) de DNIe es la Autoridad encargada de la aprobación de la presente DPC y de las Políticas de Certificación asociadas.

La AAP también es la competente para aprobar las modificaciones de dichos documentos.

## 1.6 DEFINICIONES Y ACRÓNIMOS

### 1.6.1 Definiciones

En el ámbito de esta DPC se utilizan las siguientes denominaciones:

**Activación:** es el procedimiento por el cual se desbloquean las condiciones de acceso a un clave y se permite su uso. En el caso de la tarjeta del DNIe el dato de activación es la clave personal de acceso (PIN) y/o los patrones de las impresiones dactilares (biometría)

**Autenticación:** procedimiento de comprobación de la identidad de un solicitante o titular de certificados de DNIe.

**Certificado electrónico:** un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Esta es la definición de la Ley 59/2003 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

**Certificado reconocido:** Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la

comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

**Certificados de Identidad Pública:** Emitidos como Certificados Reconocidos, vinculan una serie de datos personales del ciudadano a unas determinadas claves, para garantizar la autenticidad, integridad y no repudio. Esta información está firmada electrónicamente por la Autoridad de Certificación creada al efecto.

**Ciudadano:** toda persona física con nacionalidad española que solicita la expedición o renovación de un Documento Nacional de Identidad ante un funcionario de la Dirección General de la Policía

**Clave Pública y Clave Privada:** la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

**Clave de Sesión:** clave que establece para cifrar una comunicación entre dos entidades. La clave se establece de forma específica para cada comunicación, sesión, terminando su utilidad una vez finalizada ésta.

**Clave Personal de Acceso (PIN):** Secuencia de caracteres que permiten el acceso a los certificados

**Datos de creación de Firma (Clave Privada):** son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la Firma electrónica.

**Datos de verificación de Firma (Clave Pública):** son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la Firma electrónica.

**Directorio:** Repositorio de información que sigue el estándar X.500 de ITU-T.

**Dispositivo seguro de creación de Firma:** instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

**Documento electrónico:** conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.

**Documento de seguridad:** documento exigido por la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por la DGP como Prestador de Servicios de Certificación, para la protección de los datos de carácter personal contenidos en los Ficheros de la actividad de certificación que contienen datos personales (en adelante los Ficheros).

**Encargado del Tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento de los ficheros.

**Firma electrónica:** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal

**Firma electrónica avanzada:** es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la

integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

**Firma electrónica reconocida:** es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

**Función hash:** es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

**Hash o Huella digital:** resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

**Identificación:** procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados de DNle.

**Identificador de usuario:** conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.

**Jerarquía de confianza:** Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una AC de nivel superior garantiza la confiabilidad de una o varias de nivel inferior. En el caso de DNle, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

**Listas de Revocación de Certificados** o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

**Módulo Criptográfico Hardware de Seguridad:** módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

**Prestador de Servicios de Certificación:** persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

**Punto de Actualización del DNle:** Terminal ubicado en las Oficinas de Expedición que permite al ciudadano de forma guiada, sin la intervención de un funcionario, la realización de ciertas operaciones con el DNle (comprobación de datos almacenados en la tarjeta, renovación de los certificados de Identidad Pública, cambio de clave personal de acceso – PIN - , etc.)

**Solicitante:** persona que solicita un certificado para sí mismo

**Tercero Aceptante:** persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por DNle.

**Titular:** ciudadano para el que se expide un certificado de identidad pública

## 1.6.2 Acrónimos

**AAP:** Autoridad de Aprobación de Políticas

**AC:** Autoridad de Certificación

**AR:** Autoridad de Registro

**AV:** Autoridad de Validación.

**C:** Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**CEN:** Comité Européen de Normalisation (Comité Europeo de Normalización)

**CN:** Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**CRL:** Certificate Revocation List (Lista de Certificados Revocados)

**CWA:** CEN Workshop Agreement

**DN:** Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

**DNI:** Documento Nacional de Identidad

**DNIe:** DNI Electrónico.

**DGP:** Dirección General de la Policía

**DPC:** Declaración de Prácticas y Políticas de Certificación

**ETSI:** European Telecommunications Standard Institute

**FIPS:** Federal Information Processing Standard (Estándares del Gobierno Norteamericano para el procesamiento de la información)

**GN:** givenName (nombre). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**HSM:** Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

**IETF:** Internet Engineering Task Force (Organismo de estandarización de Internet)

**LDAP:** Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio)

**O:** Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**OCSP:** Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

**OID:** Object identifier (Identificador de objeto único)

**OU:** Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

**PKCS:** Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

**PKI:** Public Key Infrastructure (Infraestructura de Clave Pública)

**PKIX:** Grupo de trabajo del IETF (Public Key Infrastructure X509 IETF Working Group) constituido con el objeto de desarrollar las especificación relacionadas con las PKI e Internet.

**RFC:** Request For Comments (Estándar emitido por la IETF)

**SN:** surName (apellido). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

## 2. REPOSITARIOS Y PUBLICACIÓN DE INFORMACIÓN

### 2.1 REPOSITARIOS

**Para los certificados de la AC Raíz y ACs Subordinadas:**

- WEB: <http://www.dnielectronico.es/certs/ACraiz.crt>
- WEB: <http://www.dnielectronico.es/certs/ACXXX.crt><sup>1</sup>

**Para la lista de AC revocadas (ARL):**

- WEB: <http://crls.dnielectronico.es/crls/ARL.crl>

**Para la DPC:**

- <http://www.dnielectronico.es/dpc>

Desde la página se accede a los siguientes documentos (X.Y indica la versión):

- DNIe-DPC-VX.Y.pdf
- DNIe-Condiciones de aceptación-VX.Y.pdf

**Servicio de validación en línea que implementa el protocolo OCSP:**

- WEB: <http://ocsp.dnielectronico.es>

El repositorio de DNIe no contiene ninguna información de naturaleza confidencial.

### 2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El contenido de esta DPC, junto con cualquier otra información que se publique estará expuesta a título informativo en la dirección de Internet <http://www.dnielectronico.es/>. Será responsabilidad de la Dirección General de la Policía (Ministerio del Interior) la adopción de las medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

Tanto los ciudadanos como los Prestadores de servicio telemáticos podrán tener acceso de forma fiable a la DPC generada por la Autoridad de Certificación de la Dirección General de la Policía (Ministerio del Interior), accediendo a la dirección <http://www.dnielectronico.es/dpc> donde se encontrará firmada por la Autoridad de Aprobación de Políticas de la Dirección General de la Policía (Ministerio del Interior).

Las Listas de Certificados Revocados estarán firmadas electrónicamente por las AC de DNIe que las emitan y estarán disponibles únicamente para los prestadores de servicios de validación.

La información sobre el estado de los certificados se podrá consultar mediante el servicio de validación en línea que implementa el protocolo OCSP y que proporcionan los prestadores de servicios de validación recogidos en el apartado 1.3.4

---

<sup>1</sup> XXX identificador numérico de tres dígitos de la AC subordinada.

## 2.3 TEMPORALIDAD O FRECUENCIA DE PUBLICACIÓN

### ***Para los certificados de la AC Raíz y AC Subordinada:***

La publicación de los certificados de la jerarquía del DNIE se llevará a cabo con anterioridad al comienzo de la prestación del servicio en la dirección de Internet del DNIE (<http://www.dnielectrónico.es>) y a través del Boletín Oficial del Estado.

La incorporación de una nueva AC al dominio de certificación se notificará también a través de dichos medios.

### ***Para la lista de AC revocadas (ARL):***

La AC añadirá los certificados revocados a la CRL pertinente dentro del periodo de tiempo estipulado en el punto 4.9.7 *Frecuencia de emisión de CRLs*.

### ***Para la DPC:***

La DPC se publicará en el momento de su creación y se volverá a publicar en el momento en que se apruebe cualquier modificación sobre las mismas. Cuando se realicen modificaciones significativas en la DPC de DNIE, éstas se notificarán en la dirección de Internet del DNIE (<http://www.dnielectrónico.es>) y a través del Boletín Oficial del Estado

Estas notificaciones se realizarán con anterioridad a la entrada en vigor de la modificación que la haya producido.

### ***Servicio de validación en línea***

Queda fuera del alcance del presente documento regular el intercambio de información entre las Autoridades de Certificación y los Prestadores de Servicios de Validación, para que estos últimos mantengan actualizada sus bases de datos con el estado de los certificados emitidos.

## 2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la lectura a los repositorios anteriores (certificados de AC, ARLs, DPC y Políticas) es abierto, pero sólo la AAP del DNIE está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello DNIE establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.

El acceso al servicio de validación estará bajo el control de los organismos que presten dicho servicio pudiendo establecer las necesarias cautelas para evitar usos indebidos o abusivos.

### **3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS**

#### **3.1 NOMBRES**

##### **3.1.1 Tipos de nombres**

Los certificados emitidos por DNle contienen el nombre distintivo (*distinguished name* o DN) X.500 del emisor y el destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

El DN del 'issuer name' tiene los siguientes campos y valores fijos:

CN= AC DNIE XXX

OU=DNIE

O=DIRECCIÓN GENERAL DE LA POLICÍA

C=ES

Donde XXX es un identificador de tres dígitos

En el DN del 'subject name' se incluyen los siguientes campos:

CN=<APELLIDO1> <APELLIDO2>, <NOMBRE> (AUTENTICACIÓN|FIRMA)

GN=<NOMBRE>

SN=<APELLIDO1>

NÚMERO DE SERIE=<DNI> (Número personal del Documento Nacional de Identidad y carácter de verificación correspondiente al Número de Identificación Fiscal)

C=ES

##### **3.1.2 Necesidad de que los nombres sean significativos**

Las reglas definidas en el apartado anterior, garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con una identidad.

##### **3.1.3 Reglas para interpretar varios formatos de nombres**

La regla utilizada por DNle para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

La RFC 3280 ("*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*") establece que todos los certificados emitidos a partir del 31 de diciembre de 2003 deben utilizar la codificación *UTF8String* para todos los

atributos *DirectoryString* de los campos *issuer* y *subject*. En los certificados emitidos por la PKI del DNle, los atributos de dichos campos están codificados en *UTF8String*, a excepción de los campos *country* y *serialnumber*, que están codificados en *PrintableString* de acuerdo a su definición.

#### **3.1.4 Unicidad de los nombres**

El DN de los certificados no puede estar repetido. La utilización del número del DNle del ciudadano garantiza la unicidad del DN.

Los DN del certificado de autenticación y de firma se diferencian por la inclusión de los literales (AUTENTICACIÓN) y (FIRMA) en el Common Name (CN) con el objetivo de facilitar al ciudadano el reconocimiento del tipo de certificado sin necesidad de procesar alguna extensión del certificado.

#### **3.1.5 Procedimientos de resolución de conflictos sobre nombres**

Cualquier conflicto concerniente a la propiedad de nombres se resolverá según lo estipulado en el punto *9.13 Reclamaciones y jurisdicción* de esta DPC.

#### **3.1.6 Reconocimiento, autenticación y papel de las marcas registradas**

No estipulado.

### **3.2 VALIDACIÓN DE LA IDENTIDAD INICIAL**

#### **3.2.1 Medio de prueba de posesión de la clave privada**

Los dos pares de claves asociados a los certificados de identidad pública, de autenticación y firma se generan en presencia del ciudadano utilizando un dispositivo seguro de creación de firma (la tarjeta criptográfica soporte del DNI electrónico), garantizando que en todo momento las claves privadas están bajo su control. La generación de claves sólo puede ser realizada en puestos de expedición o en terminales autorizados, ambos dotados de un dispositivo identificador de terminal mediante el que se establece un canal seguro (autenticado y cifrado según CWA 14890 -1) con la tarjeta soporte del DNle. Las claves privadas se generan en la tarjeta y no pueden ser exportadas en ningún formato.

Como prueba de posesión de cada clave privada se exporta y se envía a la AC la clave pública asociada firmándola según ISO 9796-2 DS (Scheme 1) con una clave privada específica de cada tarjeta de DNle.

### 3.2.2 Autenticación de la identidad de una persona jurídica

No estipulado.

### 3.2.3 Autenticación de la identidad de una persona física

La identificación y autenticación del ciudadano para la solicitud de los Certificados de Identidad Pública y firma electrónica seguirá un proceso integrado con el registro para la expedición del Documento Nacional de Identidad de acuerdo a los procedimientos descritos en el Real Decreto que regula dicha expedición

Por lo tanto si se trata de una **primera Inscripción**, el ciudadano deberá **comparecer** en una oficina de expedición del DNIe con la documentación que se establece en el Real Decreto **1553/2005** y en el apartado 4.2 de esta DPC, acompañado de la persona que lo represente si es menor de 14 años o incapacitado.

En el caso especial de incapacitados que no puedan acudir a una Oficina de Expedición, podrán obtener su DNIe y sus Certificados de Identidad Pública, a través de un familiar que presentará en la Oficina un certificado médico oficial acreditativo de la imposibilidad, y un equipo móvil se desplazará al domicilio del ciudadano para expedirlo.

Transcurrido el período de validez del soporte físico del Documento Nacional de Identidad que para cada supuesto se contempla en el artículo 6 del Real Decreto **1553/2005**, se considerará caducado y quedarán sin efecto las atribuciones y efectos que le reconoce el ordenamiento jurídico, estando su titular obligado a proceder a la **renovación** del mismo. Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento en las oficinas de expedición del DNIe. También se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso aportar, además, los documentos justificativos que acrediten dicha variación.

El **extravío, sustracción, destrucción o deterioro** del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación.

En todos los casos anteriores la pérdida de validez del Documento Nacional de Identidad llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. Tanto la renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la revocación de los certificados vigentes y la expedición de nuevos certificados electrónicos.

A la extinción de la vigencia de los certificados electrónicos (o treinta días antes de dicha extinción), sin que medie la extinción de la vigencia del soporte (tarjeta), podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad. Para la solicitud de un nuevo certificado también deberá mediar **la presencia física** del titular en una Oficina de expedición. El ciudadano, haciendo uso de los Puntos de Actualización del DNIe habilitados en dichas oficinas y previa autenticación mediante la tarjeta y las plantillas biométricas (impresiones dactilares) capturadas durante la expedición de la Tarjeta, podrá desencadenar de forma desatendida el proceso de renovación de sus certificados. Si no fuere posible obtener la impresión dactilar de alguno de los dedos, el ciudadano deberá solicitar la renovación en un puesto de expedición atendido por un funcionario.

En el caso que haya transcurrido más de 5 años desde la identificación inicial del ciudadano (es el caso de la segunda renovación de los certificados en soportes de 10 o más años), en cumplimiento del artículo 13 de la Ley de Firma Electrónica (*“La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará ...”*) la renovación a través de los Puntos de Actualización del DNIe requerirán la personación previa del ciudadano ante un funcionario de la Oficina de Expedición a los efectos del mencionado artículo.

No se habilita por tanto ningún procedimiento de solicitud telemática de la renovación de los certificados siendo necesaria siempre la presencia física del titular en una Oficina de Tramitación.

### **3.2.4 Información no verificada sobre el solicitante**

Toda la información recabada durante la expedición anterior ha de ser verificada.

### **3.2.5 Comprobación de las facultades de representación**

Tal y como se recoge en el punto 3.2.3 la entrega del Documento Nacional de Identidad y, si procede, los certificados de identidad y firma electrónica asociados, deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o incapaz se llevará a cabo en presencia de la persona que tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas.

### **3.2.6 Criterios para operar con AC externas**

A la entrada en vigor de la presente DPC no se contempla el establecimiento de relaciones de confianza con Prestadores de Servicios de Certificación (PSC) externos.

## **3.3 IDENTIFICACIÓN Y AUTENTICACIÓN EN LAS PETICIONES DE RENOVACIÓN DE CLAVES Y CERTIFICADOS**

### **3.3.1 Identificación y autenticación por una renovación de claves de rutina**

Se han de distinguir dos casos:

- Renovación de claves sin renovación del soporte físico (tarjeta): la identificación y autenticación se hará mediante los certificados de identidad pública, aun no estando estos en vigor, y mediante las plantillas biométricas (impresiones dactilares) capturadas durante la expedición de la Tarjeta. La renovación se deberá efectuar en los terminales (Puntos de Actualización del DNIe) establecidos a tal efecto en las Oficinas de Expedición del Documento Nacional de Identidad. Si no fuese posible obtener la impresión dactilar de

alguno de los dedos, el ciudadano deberá solicitar la renovación en un puesto de expedición atendido por un funcionario. Es de aplicación lo establecido en el apartado 3.2.3

- Renovación de claves por caducidad o sustitución del soporte físico (tarjeta): Se hará de igual forma que en la primera inscripción, siendo necesaria la presencia física del titular, tal como recoge el apartado 3.2.3.

No se habilita por tanto ningún procedimiento para solicitar de forma telemática la renovación de los certificados siendo necesaria en todos los casos la presencia física del titular.

### **3.3.2 Identificación y autenticación para una renovación de claves tras una revocación**

Será de aplicación lo contemplado en el punto anterior, tanto si la revocación ha sido acompañada de una sustitución del soporte como si no.

## **4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS**

En este capítulo se recogen los requisitos operacionales para el ciclo de vida de los certificados de identidad pública (autenticación y firma electrónica), ciclo de vida que está totalmente integrado con el de la tarjeta soporte del DNI. La emisión del documento y de los certificados asociados se realizará en una sola visita a la oficina expedidora del DNI.

### **4.1 SOLICITUD DE CERTIFICADOS**

#### **4.1.1 Quién puede efectuar una solicitud**

Todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad, siendo obligatoria su obtención por los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.

También el DNIe, como recoge el Real Decreto **1553/2005**, permitirá a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento.

Sólo se podrá solicitar la expedición del nuevo Documento Nacional de Identidad, con la incorporación de los dispositivos de firma electrónica, en aquellos equipos que lo permitan dentro del marco del proceso de sustitución del actual documento. La Dirección

General de la Policía programará y organizará, temporal y territorialmente el proceso de sustitución de las tarjetas soporte del Documento Nacional de Identidad emitidas con anterioridad a la entrada en vigor del Real Decreto **1553/2005** de 23 de Diciembre por el nuevo Documento Nacional de Identidad, pudiendo establecerse por razones de interés público programaciones especiales para determinados colectivos.

#### **4.1.2 Registro de las solicitudes de certificados**

La obtención de los certificados de identidad y firma electrónica está ligada a la de la tarjeta soporte del DNI electrónico

El ciudadano que desee solicitar por primera vez su DNIE y por tanto los Certificados asociados deberá acudir a una Oficina de Expedición del DNIE. La relación de equipos fijos de expedición está accesible en el sitio web: [www.dnielectronico.es](http://www.dnielectronico.es). A aquellas localidades que no dispongan de un equipo fijo de expedición, podrá desplazarse un Equipo Móvil que con carácter general se instalará en las oficinas municipales. Los ciudadanos residentes en estas localidades y en las localidades próximas, podrán obtener o renovar el DNIE (y por tanto los certificado asociados) aportando los mismos documentos que en los equipos fijos.

Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los siguientes documentos:

- a) Certificación literal de nacimiento expedida por el Registro Civil correspondiente. A estos efectos únicamente serán admitidas las certificaciones expedidas con una antelación máxima de tres meses a la fecha de presentación de la solicitud de expedición del Documento Nacional de Identidad
- b) Una fotografía reciente en color del rostro del solicitante, tamaño 32 por 26 milímetros, con fondo uniforme claro liso, tomada de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.
- c) Certificado de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del Documento Nacional de Identidad.
- d) Los españoles residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes.

Excepcionalmente, en los supuestos en que, por circunstancias ajenas al solicitante, no pudiera ser presentado alguno de los documentos anteriores, y siempre que se acrediten por otros medios, suficientes a juicio del responsable del órgano encargado de la expedición, los datos que consten en tales documentos, se le podrá expedir un Documento Nacional de Identidad con una validez de un año.

En el momento de la solicitud, al interesado se le recogerá la imagen digitalizada de la firma manuscrita así como las impresiones dactilares de los dedos índices de ambas manos. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de

ambos, por mutilación o defecto físico de los mismos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden: medio, anular, auricular o pulgar. Si se careciese de todos ellos, se hará constar en el lugar del soporte destinado a tal fin el motivo por el que no aparece dicha impresión.

Finalizada la fase de gestión documental y la personalización física de la tarjeta, comenzará la fase de personalización lógica con la carga de datos en el chip de la tarjeta soporte (datos de filiación, imágenes digitalizadas de fotografía y de firma manuscrita, plantillas de las impresiones dactilares de un dedo de cada mano) y con la generación de los pares de claves asociados a los certificados de identidad y firma electrónica.

La generación de claves se realizará en la tarjeta y en presencia del titular, tras la habilitación de una clave personal de acceso –PIN- aleatoria que se entrega al ciudadano en forma de sobre ciego. Dicha clave de acceso es confidencial, personal e intransferible y es el parámetro que protege sus claves privadas permitiendo la utilización de los certificados en los servicios ofrecidos a través de una red de comunicaciones. La clave persona de acceso – PIN - podrá ser cambiada por otra de la elección del ciudadano utilizando las herramientas que se describen más adelante en esta DPC.

Una vez generadas las claves, se enviará una solicitud de certificación para cada par de claves (autenticación y firma), que irá acompañada de la prueba de posesión de la clave privada tal y como se describe en punto 3.2.1.

Todos los datos relacionados con el registro de certificación quedarán registrados en el sistema central, firmados con un certificado de firma electrónica que tiene como titular al funcionario responsable del puesto de expedición.

## **4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS**

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

Las funciones de identificación y autenticación descritas en el punto 3.2.3 las realizan los funcionarios y personal encargado de la operación de los Equipos de Expedición del DNLe.

Estos funcionarios desempeñan el rol de operador de registro, disponiendo de un dispositivo seguro de creación de firma (tarjeta de funcionario) para el control de acceso a la aplicación de expedición y control de integridad y no repudio de las operaciones y transacciones realizadas.

### **4.2.2 Aprobación o denegación de las solicitudes de certificados**

Solo se privará del derecho a la expedición de un DNLe y/o a los dispositivos de creación de firma que incorpora, en los casos y forma establecidos por el Real Decreto que regula su expedición y otras Leyes de aplicación.

Hacer notar que tras la aprobación de esta DPC y la puesta en marcha del sistema, el nuevo DNI sólo podrá ser solicitado en aquellos equipos que hayan reemplazado el sistema anterior dentro del marco del proceso de sustitución del actual documento.

Una vez tramitada la solicitud de certificación por parte del funcionario encargado de la expedición, la emisión del certificado tendrá lugar una vez que la AC destinataria de la petición haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación.

El sistema garantiza que la petición:

- Procede de un puesto de expedición autorizado (tarjeta de identificación de puesto que contiene un par de claves y un certificado de componente asociado al puesto)
- Procede de un funcionario o personal contratado con capacidad de expedir DNIE (tarjeta de identificación de funcionario que contiene un par de claves y un certificado de autenticación y un par de claves y un certificado de firma electrónica)
- Procede de una tarjeta de DNIE válida (todas las tarjetas soporte de DNIE dispondrán de un par de claves y un certificado de componente vinculado al número de serie del chip)
- Consta de toda la información necesaria para habilitar los campos y extensiones del certificado de acuerdo con los perfiles definidos.

Si alguna de las verificaciones no llega a buen término, la AC podrá rechazar la solicitud de certificación.

### **4.2.3 Plazo para la tramitación de las solicitudes de certificados**

No estipulado.

## **4.3 EMISIÓN DE CERTIFICADOS**

### **4.3.1 Actuaciones de la AC durante la emisión de los certificados**

La emisión de los certificados implica la autorización definitiva de la solicitud por parte de la AC. Después de la aprobación de la solicitud se procederá a la emisión de los certificados de forma segura y se pondrán los certificados a disposición del ciudadano insertándolos en la tarjeta soporte de DNIE, como etapa final en el proceso de personalización lógica de la misma.

Los dos certificados, autenticación y firma, son emitidos por la misma AC, cuyo certificado se inserta también en la tarjeta para facilitar la construcción de la cadena de confianza en los procesos de firma.

Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados, ya que ésta implica la emisión de nuevos certificados.

En la emisión de los certificados la AC:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada
- Protege la confidencialidad e integridad de los datos de registro
- Incluye en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003.

Cuando una AC del la PKI del DNle emita un certificado de acuerdo con una solicitud de certificación efectuará las notificaciones que se establecen en el apartado 4.3.2 del presente capítulo.

Todos los certificados iniciarán su vigencia en el momento de su emisión, salvo que se indique en los mismos una fecha y hora posterior a su entrada en vigor, que no será posterior al día natural desde su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.

#### **4.3.2 Notificación al solicitante de la emisión por la AC del certificado**

El solicitante conocerá la emisión efectiva de los certificados de identidad pública con la entrega del DNle.

La entrega del documento nacional de identidad y de los certificados asociados deberá realizarse personalmente a su titular. En el momento de la entrega del documento nacional de identidad, y a través del documento de aceptación de condiciones, se indicará al ciudadano cómo obtener la presente DPC así como el resto de información a que se refiere el artículo 18.b) de la Ley 59/2003, de 19 de diciembre.

### **4.4 ACEPTACIÓN DEL CERTIFICADO**

#### **4.4.1 Forma en la que se acepta el certificado**

Tal y como recoge el Real Decreto **1553/2005** la activación de las funcionalidades electrónicas del DNI tendrá carácter voluntario, por lo que el ciudadano podrá solicitar la revocación de los certificados emitidos como parte del proceso de expedición.

Si el usuario no manifiesta la intención de revocar dichos certificados tras la expedición, se dará por confirmada la aceptación de los mismos, así como de sus condiciones de uso, independientemente que se hayan obtenido tras la primera inscripción, en las renovaciones presenciales o en la expedición de duplicados.

#### 4.4.2 Publicación del certificado por la AC

No estipulado: los certificados de ciudadano no se publicarán en ningún repositorio de acceso libre.

#### 4.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades

No procede.

### 4.5 PAR DE CLAVES Y USO DEL CERTIFICADO

#### 4.5.1 Uso de la clave privada y del certificado por el titular

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta DPC y de acuerdo con lo establecido en los campos 'Key Usage' (Uso de la Clave) de los certificados. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en esta DPC (apartados 1.4.1 y 1.4.2) y sólo para lo que éstas establezcan.

Tras la extinción de la vigencia o la revocación del certificado el titular deberá dejar de usar la clave privada asociada.

Los Certificados de Identidad Pública, emitidos por la Dirección General de la Policía (Ministerio del Interior) tendrán como finalidad:

- **Certificado de Autenticación:** garantizar electrónicamente la identidad del ciudadano.
- **Certificado de Firma:** permitir la firma electrónica reconocida de documentos.

#### 4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes

Los Terceros Aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece esta DPC y de acuerdo con lo establecido en el campo 'Key Usage' del certificado.

Los Terceros Aceptantes han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos.

## **4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES**

### **4.6.1 Circunstancias para la renovación de certificados sin cambio de claves**

No procede: Todas las renovaciones de certificados realizadas en el ámbito de esta DPC se realizarán con cambio de claves.

## **4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES**

### **4.7.1 Circunstancias para una renovación con cambio claves de un certificado**

Todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves.

Con carácter general la tarjeta soporte físico Documento Nacional de Identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

- Cinco años, cuando el titular no haya cumplido los treinta al momento de la expedición o renovación
- Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.
- Permanente cuando el titular haya cumplido los setenta años y a personas mayores de treinta años que acrediten la condición de gran inválido.
- Por un año, en ciertos casos excepcionales contemplados en el Real Decreto que regula la expedición del DNIE (como, por ejemplo, cuando el ciudadano no pueda aportar en el momento de la expedición parte de la documentación solicitada)

Por otro lado los certificados electrónicos reconocidos incorporados al DNIE tendrán un período de vigencia de treinta meses, siempre que este periodo no supere el del soporte físico, en cuyo caso, la fecha de caducidad del certificado vendrá determinada por la del soporte.

En este contexto se pueden dar los siguientes escenarios de renovación con cambio de claves de un certificado:

- Renovación de los certificados por renovación del soporte por caducidad del mismo o en los supuestos de variación de los datos que se recogen.

- Renovación de los certificados por expedición de duplicado del soporte. Es el caso de renovación por sustracción, extravío, destrucción, deterioro o incorrecto funcionamiento del chip del DNI.
- Renovación por caducidad de los certificados sin que medie un cambio de soporte. Esta solicitud podrá realizarse desde los Puntos de Actualización del DNIE habilitados en las Oficinas de expedición del DNIE, en un periodo de tiempo que abarca desde treinta días antes de la fecha de caducidad hasta cualquier instante posterior a dicha fecha siempre que el soporte físico (la tarjeta DNIE) no este dentro del periodo habilitado para solicitar su renovación.

#### **4.7.2 Quién puede pedir la renovación de un certificado**

El proceso de renovación de los Certificados sin que medie una renovación del soporte físico deberá ser solicitado de forma voluntaria y por iniciativa del ciudadano.

En los casos de caducidad del soporte del DNIE, el titular está obligado a proceder a la renovación del mismo, estando acompañado el proceso de renovación del soporte de la renovación de los certificados y las claves (renovación con cambio de claves). La renovación en los supuestos de variación de datos tiene las mismas implicaciones.

Por otro lado, el extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que vendrá acompañado de la revocación automática de los certificados vigentes y la emisión de unos nuevos (renovación con cambio de claves).

No obstante, tal y como recoge el RD 1553/2005, “la activación del dispositivo de creación de firma tendrá carácter voluntario”, por lo que el ciudadano podrá solicitar la revocación de los certificados como parte del proceso de renovación del soporte.

La DGP como Órgano que tiene atribuidas las competencias del DNIE se reserva el derecho de denegar la solicitud de renovación de los certificados de Identidad Pública (autenticación y firma) cuando el número de revocaciones sin causa justificada de certificados asociados a un mismo soporte físico (tarjeta DNIE) sea superior a 3 en el caso de soportes de 5 años y superior a 5 en el resto de casos.

#### **4.7.3 Tramitación de las peticiones de renovación con cambio de claves**

Se dan los siguientes escenarios:

- Cuando medie la renovación del soporte físico por caducidad o variación de datos.  
Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento, que deberá abonar la tasa correspondiente y aportar una fotografía con las mismas características señaladas en el proceso de primera expedición. También se le recogerán las impresiones dactilares y la imagen digitalizada de la firma manuscrita.

Antes de proceder a la renovación de las claves y certificados se procederá a la revocación automática de los vigentes.

Al entregar el Documento renovado, se procederá a la retirada del anterior para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita.

Todo el proceso deberá ser realizado en un puesto de expedición atendido por un funcionario.

- o En los casos de extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad.

Todos ellos conllevarán la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación prevista en el caso anterior. La validez de estos duplicados será la misma que tenían los Documentos a los que sustituyen, salvo que éstos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.

En los casos que se disponga de documento, se procederá a su retirada para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita. Antes de proceder a la renovación de las claves y certificados se procederá a la revocación automática de los vigentes.

Todo el proceso deberá ser realizado en un puesto de expedición atendido por un funcionario.

- o Cuando sólo sea necesaria la renovación de los certificados y no del soporte.

Desde treinta días antes de la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente. La tramitación se llevará a cabo, tras la autenticación del ciudadano mediante sus impresiones dactilares, desde los Puntos de Actualización del DNIe emplazados en los lugares controlados por la Unidad de Documentación de Españoles de la Comisaría de Extranjería y Documentación. Los certificados tendrán como fecha de entrada en vigor el instante en que haya sido generado y como periodo de validez 30 meses (sin superar el periodo de validez del soporte físico). Los certificados vigentes hasta el momento serán eliminados de la tarjeta sin solicitar su revocación.

En los tres casos cuando el sistema de expedición de la Dirección General de la Policía (Ministerio del Interior) reciba la solicitud del ciudadano en debida forma, y tras comprobar su identidad, se procederá a la generación de nuevas claves criptográficas y a la emisión de nuevos Certificados de Identidad que tendrán como fecha de entrada en vigor el instante en que han sido generados, procediéndose en este mismo proceso al borrado de las claves y certificados anteriores.

Es de aplicación lo recogido en el apartado 4.3 respecto a la emisión de estos certificados.

#### **4.7.4 Notificación de la emisión de nuevos certificado al titular**

La notificación se hace con la entrega del nuevo DNIe o mediante la comunicación de la finalización satisfactoria del proceso de renovación cuando no se cambie de soporte.

#### **4.7.5 Forma de aceptación del certificado con nuevas claves**

En el caso de renovación de los certificados tras un cambio en el soporte, si el usuario no manifiesta la intención de revocar dichos certificados, se dará por confirmada la aceptación de los mismos, así como de sus condiciones de uso.

En los casos de renovación de los certificados en los Puntos de Actualización del DNIe, el propio acto de renovación conlleva la aceptación implícita de los certificados.

#### **4.7.6 Publicación del certificado con las nuevas claves por la AC**

Los certificados no se publican.

#### **4.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades**

No estipulado

### **4.8 MODIFICACIÓN DE CERTIFICADOS**

#### **4.8.1 Causas para la modificación de un certificado**

Todas las circunstancias que obligarían a efectuar modificaciones en los certificados emitidos a un ciudadano por variación de los datos contenidos en el mismo, también obligarían al cambio del soporte físico por lo se tratarán como una renovación del soporte por variación de datos, siendo de aplicación los apartados anteriores.

### **4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS**

La revocación y suspensión de los Certificados de Identidad Pública son mecanismos a utilizar en el supuesto de que por alguna causa establecida en esta DPC se deje de confiar en dichos Certificados antes de la finalización del período de validez originalmente previsto.

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su fecha de caducidad. El efecto de la revocación de un certificado es la pérdida de validez del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia la revocación de un certificado inhabilita el uso legítimo del mismo por parte del titular.

Como regla general la pérdida de validez del soporte del Documento Nacional de Identidad (tarjeta) llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. De este modo la renovación del Documento Nacional de Identidad por variación de datos o la expedición de duplicados del mismo implicará, a su vez, la revocación de los certificados vigentes y la expedición de nuevos certificados electrónicos.

No se contempla la revocación individual de uno de los certificados del DNIE, sino que se revocarán simultáneamente los dos certificados.

#### **4.9.1 Causas para la revocación**

Los certificados de identidad pública (autenticación y firma) pueden ser revocados por:

- Sustracción, extravío, destrucción o deterioro del DNIE soporte del Certificado.
- Tras la renovación por variación de los datos.
- Incapacidad sobrevenida o fallecimiento del titular del DNIE
- Inexactitudes graves en los datos aportados por el ciudadano para la obtención del DNI, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado no se adecuen a la realidad.
- Compromiso de las claves privadas del ciudadano, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de la clave personal de acceso (PIN) que permite la activación de dichas claves privadas, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por entidad ajena a su titular.
- Compromiso de la clave privada de la Autoridad de Certificación de la Dirección General de la Policía (Ministerio del Interior) emisora del certificado de ciudadano por cualquiera de las causas mencionadas en el punto anterior.
- Por incumplimiento por parte de la Autoridad de Certificación, de los funcionarios responsables de la expedición o del ciudadano de las obligaciones establecidas en esta DPC.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta tal punto que se ponga en duda la fiabilidad de la Identidad Pública Digital.
- Declaración de que el ciudadano no tiene capacidad de firma (pródigo)
- Por resolución judicial o administrativa que lo ordene conforme a derecho.
- Por voluntad del ciudadano titular.

En relación con las anteriores causas de revocación se debe tener en consideración lo siguiente:

- La decisión de revocar un certificado de oficio o por resolución judicial será comunicada con carácter previo o simultáneo por la Autoridad de Certificación de la Dirección General de la Policía (Ministerio del Interior) al ciudadano

mediante correo ordinario y, en caso de disponer de la dirección electrónica, mediante e-mail firmado electrónicamente

- A través de esta DPC se pone en conocimiento del ciudadano que todos los procedimientos relacionados con el DNLe que implican el cambio del soporte físico van acompañados de la revocación de los certificados que contiene dicho soporte.
- Con el resto de causas que pueden desencadenar la revocación de un certificado, siempre media la solicitud del ciudadano.

La revocación de un Certificado tendrá como consecuencia la notificación a terceros que dicho certificado ha sido revocado, siempre que se solicite la verificación del mismo a través de uno de los prestadores de servicios de validación.

#### **4.9.2 Quién puede solicitar la revocación**

Estará legitimado para solicitar la revocación de un certificado:

- El ciudadano interesado cuando concurra cualquiera una de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.
- Un tercero aceptante cuando tenga constancia demostrable que un certificado de identidad pública ha sido empleado con fines fraudulentos.
- La propia Dirección General de la Policía (Ministerio del Interior) como Autoridad de Certificación cuando tenga conocimiento del robo o extravío del DNLe o de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.

#### **4.9.3 Procedimiento de solicitud de revocación**

Las solicitudes de revocación se realizarán personalmente por el interesado ante cualquier equipo expedidor del DNLe, cualquier oficina de la Dirección General de la Policía o de los Cuerpos y Fuerzas de Seguridad, sin perjuicio de cualquier otro procedimiento que pudiera establecerse por la Dirección General de la Policía a estos efectos.

Dado que el titular del Documento está obligado a la custodia y conservación del mismo, en los casos que el motivo de revocación sea la pérdida de validez del soporte (por pérdida, sustracción, destrucción o deterioro), el titular deberá comunicar inmediatamente tales hechos a la Dirección General de la Policía por los procedimientos y medios que al efecto habilite la misma y que serán publicados en [www.dnielectronico.es](http://www.dnielectronico.es).

Esta DPC no contempla ningún procedimiento para solicitar de forma telemática la revocación de los certificados siendo necesaria en todos los casos la presencia física del titular.

La DGP como órgano que tiene atribuida la gestión de la PKI del DNLe podrá solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del suscriptor, o cualquier otro hecho que recomendará emprender dicha acción.

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

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación.

#### **4.9.5 Plazo en el que la AC debe resolver la solicitud de revocación**

La solicitud de revocación de un certificado de firma reconocida debe ser atendida con la máxima celeridad, sin que en ningún caso su tratamiento pueda ser superior a 24 horas.

#### **4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes**

La verificación de las revocaciones es obligatoria para cada uso de los certificados de identidad pública. El procedimiento ordinario de comprobación de la validez de un certificado será la consulta a los Prestadores de Servicios de Validación, los cuales mediante protocolo OCSP indicarán el estado del certificado.

#### **4.9.7 Frecuencia de emisión de CRLs**

La PKI del DNIE no publica CRLs en repositorios de acceso libre. Estas únicamente están disponibles como medio para intercambiar información de estado de los certificados con los Prestadores de Servicios de Validación.

DNIE publicará una nueva CRL en su repositorio en el momento que se produzca cualquier revocación, y, en último caso, a intervalos no superiores a 24 horas (aunque no se hayan producido modificaciones en la CRL) para las generadas por ACs subordinadas y de 3 meses para las ARL generadas por la AC Raíz.

#### **4.9.8 Tiempo máximo entre la generación y la publicación de las CRL**

Según lo estipulado en 4.9.7

#### **4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados**

Existe una red de Autoridades de Validación que, mediante el protocolo OCSP, permite verificar el estado de los certificados.

Las direcciones de acceso a la Autoridad de Validación quedan reflejadas en el apartado *2.1 Repositorio*.

#### **4.9.10 Requisitos de comprobación en-línea de revocación**

En el caso de utilizar la(s) Autoridad(es) de Validación el Tercero Aceptante debe de disponer de un software que sea capaz de operar con el protocolo OCSP para obtener la información sobre el certificado.

#### **4.9.11 Otras formas de divulgación de información de revocación disponibles**

No estipulado

#### **4.9.12 Requisitos especiales de renovación de claves comprometidas**

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.

#### **4.9.13 Circunstancias para la suspensión**

No se contempla

#### **4.9.14 Quién puede solicitar la suspensión**

No se contempla

#### **4.9.15 Procedimiento para la solicitud de suspensión**

No se contempla

#### **4.9.16 Límites del periodo de suspensión**

No se contempla

### **4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS**

#### **4.10.1 Características operativas**

Para la validación del DNle se dispone de varios prestadores de Servicios de Validación que proporcionan información sobre el estado de los certificados emitidos por la

jerarquía de certificación del DNle. Se trata de un servicio de validación en línea (Autoridad de Validación, AV) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560. Mediante el uso de ese protocolo se determina el estado actual de un certificado electrónico sin requerir las CRLs. Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su BBDD, ofrece una respuesta sobre el estado del certificado vía HTTP.

#### **4.10.2 Disponibilidad del servicio**

El servicio de validación está disponible de forma ininterrumpida todos los días del año.

#### **4.10.3 Características adicionales**

Para hacer uso del Servicio de validación en línea es responsabilidad del Tercero Aceptante disponer de un Cliente OCSP que cumpla la RFC 2560.

### **4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN**

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas recogidas en el apartado 4.9.1.
- Caducidad de la vigencia del certificado.

### **4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES**

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

La tarjeta soporte del DNle es un dispositivo seguro de creación de firma certificado EAL4+. Los datos de creación de firma (las claves privadas) se generan dentro de la tarjeta y no pueden ser exportadas en ningún caso.

No se efectúa por tanto archivo de la clave privada de los certificados.

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

No estipulado.

## **5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES**

### **5.1 CONTROLES FÍSICOS**

Los aspectos referentes a los controles de seguridad física se encuentran recogidos en detalle en la documentación que la Dirección General de la Policía ha desarrollado a tal efecto. En este apartado se van a recoger las medidas adoptadas más relevantes.

#### **5.1.1 Ubicación física y construcción**

Los edificios donde se encuentra ubicada la infraestructura de DNIE disponen de medidas de seguridad de control de acceso, de forma que sólo se permite la entrada a los mismos a las personas debidamente autorizadas.

Todas las operaciones críticas de DNIE se realizan en recintos físicamente seguros, con niveles de seguridad específicos para los elementos más críticos y con vigilancia durante las 24 horas al día, los 7 días a la semana. Estos sistemas están separados de otros de la DGP, de forma que sólo el personal autorizado pueda acceder a ellos.

Los Centros de Proceso de Datos de DNIE cumplen los siguientes requisitos físicos:

- a) Están alejados de salidas de humos para evitar posibles daños por incendios en otras plantas.
- b) Ausencia de ventanas al exterior del edificio.
- c) Cámaras de vigilancia en las áreas de acceso restringido.
- d) Control de acceso basado en tarjeta y biometría.
- e) Sistemas de protección y prevención de incendios: detectores, extintores, formación del personal para actuar ante incendios, etc.
- f) Existencia de mamparas transparentes, limitando las distintas zonas, que permitan observar las salas desde pasillos de acceso, para detectar intrusiones o actividades ilícitas en su interior.
- g) Protección del cableado contra daños e interceptación tanto de la transmisión de datos como de telefonía.

#### **5.1.2 Acceso físico**

Se dispone de un completo sistema de control de acceso físico de personas a la entrada y a la salida que conforman varios niveles de control. Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

Los sistemas de DNIE estarán físicamente separados de otros sistemas de la DGP de forma que únicamente el personal autorizado pueda acceder a ellos, y se garantice la independencia de los otros sistemas informáticos.

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

### **5.1.3 Alimentación eléctrica y aire acondicionado**

Las salas donde se ubican los equipos de la infraestructura de DNIE disponen de suministro de electricidad y aire acondicionado adecuado a los requisitos de los equipos en ellas instalados. La infraestructura está protegida contra caídas de tensión o cualquier anomalía en el suministro eléctrico. Las instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. El apagado de los equipos sólo se producirá en caso de fallo de los sistemas de generación autónoma de alimentación.

### **5.1.4 Exposición al agua**

Se han tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado, disponiendo de detectores de inundación y sistemas de alarma apropiados al entorno.

### **5.1.5 Protección y prevención de incendios**

Las salas donde se ubican los activos de la infraestructura del DNIE disponen de los medios adecuados – sistemas automáticos de detección y extinción de incendios- para la protección de su contenido contra incendios.

El cableado se encuentra en falso suelo o falso techo y se dispone de los medios adecuados - detectores en suelo y techo- para la protección del mismo contra incendios.

### **5.1.6 Sistema de almacenamiento**

DNIE ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

DNIE ha dispuesto planes de copia de respaldo, los mismos que para el resto de los sistemas de información de la DGP, de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.

Los soportes de información sensible se almacenan de forma segura en armarios ignífugos y cajas fuertes, según el tipo de soporte y la clasificación de la información en ellos contenida. Estos armarios se encuentran en diversas dependencias para eliminar riesgos asociados a una única ubicación.

El acceso a estos soportes está restringido a personal autorizado.

### 5.1.7 Eliminación de los soportes de información

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

La eliminación de soportes, tanto papel como magnéticos, se realiza mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte. En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

### 5.1.8 Copias de seguridad fuera de las instalaciones

DNiE dispone de copias de seguridad en locales propios que reúnen las medidas precisas de seguridad y con una separación física adecuada.

## 5.2 CONTROLES DE PROCEDIMIENTO

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se incluye una parte de la misma.

DNiE procura que toda la gestión, tanto la relativa a los procedimientos operacionales como a la de administración, se lleve a cabo de forma segura, conforme a lo establecido en este documento, realizando auditorías periódicas. (Véase el capítulo 8 *Auditorías de Cumplimiento y otros Controles de Conformidad*).

Asimismo, se ha diseñado una segregación de funciones para evitar que una sola persona pueda conseguir el control total de la infraestructura.

### 5.2.1 Roles responsables del control y gestión de la PKI

Se distinguen los siguientes roles para la operación y gestión del sistema:

- **Administradores de Sistema:** Conjunto de usuarios autorizados a realizar ciertas tareas relacionadas con la instalación, configuración y mantenimiento de las entidades de la PKI, pero con acceso limitado a la información relacionada con los parámetros de seguridad. Responsable del funcionamiento de los sistemas que componen la PKI, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de datos, del repositorio de información y de los sistemas operativos.
- **Administradores HSM (Modulo Seguridad Hardware):** Encargados de la definición de claves de administración del HSM, de su custodia, de su configuración y puesta en marcha.
- **Audidores de Sistema:** Autorizados a consultar archivos, trazas y logs de auditoría de las entidades de la PKI.

- **Coordinador de Seguridad:** responsable de la definición y verificación de todos los procedimientos de seguridad tanto física como informática.
- **Generador de ARLs:** encargado de la emisión manual de las Authority Revocation Lists con la periodicidad establecida en la DPC.
- **Oficiales de Registro:** Son los responsables de solicitar en nombre de las entidades finales la generación/revocación de los certificados. Los funcionarios y personal contratado responsable de un puesto de expedición desempeñarán el rol de oficial de registro.
- **Oficiales de Seguridad:** Los usuarios pertenecientes a este grupo tienen la responsabilidad global de administrar la implementación de las políticas y prácticas de seguridad.
- **Operadores de Sistema:** Usuarios encargados de realizar tareas básicas del día a día como por ejemplo, ejecutar los procesos de backup y recuperación.
- **Operadores HSM:** Encargados de configurar el acceso al HSM por parte de las aplicaciones, de la inicialización del token PKCS#11, de asistir en las tareas de exportación e importación del material criptográfico, etc
- **Usuarios HSM:** encargados de la explotación de los servicios criptográficos del HSM

### 5.2.2 Número de personas requeridas por tarea

Se requiere un mínimo de tres personas con capacidad profesional suficiente para realizar las tareas correspondientes al **Oficial de Seguridad** y tres personas para las correspondientes a las de **los Administradores del HSM**

### 5.2.3 Identificación y autenticación para cada usuario

Los Administradores y Operadores de HSM se identifican y autentican en los HSM mediante técnicas de secreto compartido en tarjetas criptográficas específicas de los HSM.

El resto de usuarios autorizados de DNIE se identifican mediante certificados electrónicos emitidos por la propia infraestructura del DNIE y se autentican por medio de tarjetas criptográficas.

La autenticación se complementa con las correspondientes autorizaciones para acceder a determinados activos de información o sistemas del DNIE.

### 5.2.4 Roles que requieren segregación de funciones

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos roles marcados como "incompatibles":

- Incompatibilidad entre el rol auditor (i.e. auditor de sistema) y cualquier otro rol.

- Incompatibilidad entre los roles administrativos (coordinador de seguridad, administrador de sistema y oficial de registro)
- Incompatibilidad entre los administradores y los operadores del HSM
- Incompatibilidad entre el oficial de seguridad y el administrador del HSM

## **5.3 CONTROLES DE PERSONAL**

### **5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales**

Todo el personal que preste sus servicios en el ámbito de la DNle deberá poseer el conocimiento, experiencia y formación suficientes, para el mejor cometido de las funciones asignadas.

Para ello, la DGP llevará a cabo los procesos de selección de personal que estime precisos con objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

### **5.3.2 Procedimientos de comprobación de antecedentes**

Conforme a la normativa general de la Administración del Estado

### **5.3.3 Requerimientos de formación**

Según los procedimientos establecidos por la DGP.

En particular, el personal relacionado con la explotación de la PKI, recibirá la formación necesaria para asegurar la correcta realización de sus funciones. Se incluyen en la formación los siguientes aspectos:

- Entrega de una copia de la Declaración de Prácticas y Políticas de Certificación.
- Concienciación sobre la seguridad física, lógica y técnica
- Operación del software y hardware para cada papel específico.
- Procedimientos de seguridad para cada rol específico.
- Procedimientos de operación y administración para cada rol específico.
- Procedimientos para la recuperación de la operación en caso de desastres.

### **5.3.4 Requerimientos y frecuencia de actualización de la formación**

Según los procedimientos establecidos por la DGP.

### **5.3.5 Frecuencia y secuencia de rotación de tareas**

No estipulado

### **5.3.6 Sanciones por actuaciones no autorizadas**

La comisión de acciones no autorizadas será calificada como falta laboral y sancionada conforme a lo preceptuado (reglamento del Cuerpo Nacional de Policía y Legislación General de la Función Pública)

Se considerarán acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

Si se produce alguna infracción, se suspenderá el acceso de las personas involucradas a todos los sistemas de información del DNIE de forma inmediata al conocimiento del hecho.

### **5.3.7 Requisitos de contratación de terceros**

Se aplicará la normativa general de la DGP para las contrataciones.

### **5.3.8 Documentación proporcionada al personal**

Se facilitará el acceso a la normativa de seguridad de obligado cumplimiento junto con la presente DPC.

## **5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD**

### **5.4.1 Tipos de eventos registrados**

Se registrarán todos los eventos relacionados con la operación y gestión del sistema, así como los relacionados con la seguridad del mismo, entre otros:

- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs

- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal
- Cambios en las claves de la Autoridad de certificado
- Cambios en las políticas de emisión de certificados y en la presente DPC
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor
- Informes de compromisos y discrepancias
- Registros de acceso físico
- Acontecimientos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste
- La ceremonia de generación de claves y las bases de datos de gestión de claves

Las operaciones se dividen en eventos, por lo que se guarda información sobre uno o más eventos para cada operación relevante. Los eventos registrados poseen, como mínimo, la información siguiente:

**Categoría:** Indica la importancia del evento.

- Informativo: los eventos de esta categoría contienen información sobre operaciones realizadas con éxito.
- Marca: cada vez que empieza y termina una sesión de administración, se registra un evento de esta categoría.
- Advertencia: indica que se ha detectado un hecho inusual durante una operación, pero que no provocó que la operación fallara (p.ej. una petición de lote denegada).
- Error: indica el fallo de una operación debido a un error predecible (p.ej. un lote que no se ha procesado porque la AR pidió una plantilla de certificación para la cual no estaba autorizada).
- Error Fatal: indica que ha ocurrido una circunstancia excepcional durante una operación (p.ej. una tabla de base de datos a la que no se puede acceder).

**Fecha:** Fecha y hora en la que ocurrió el evento.

**Autor:** Nombre distintivo de la Autoridad que generó el evento.

**Rol:** Tipo de Autoridad que generó el evento.

**Tipo evento:** Identifica el tipo del evento, distinguiendo, entre otros, los eventos criptográficos, de interfaz de usuario, de librería.

**Módulo:** Identifica el módulo que generó el evento. Los posibles módulos son:

- AC.
- AR.
- Repositorio de información.
- Librerías de control de almacenamiento de información.

**Descripción:** Representación textual del evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyos valores variarán dependiendo de los datos sobre los que se ejecutó la operación. Algunos ejemplos de los parámetros que se incluyen para la descripción del evento "Certificado generado" son: el número de serie, el nombre distintivo del titular del certificado emitido y la plantilla de certificación que se ha aplicado.

#### **5.4.2 Frecuencia de procesado de registros de auditoría**

Los registros se analizarán siguiendo procedimientos manuales y automáticos cuando sea necesario, aunque se establecen tres niveles de auditorías de control de los eventos registros con una frecuencia semanal, mensual y anual.

#### **5.4.3 Periodo de conservación de los registros de auditoría**

La información generada por los registros de auditoría se mantiene en línea hasta que es archivada. Una vez archivados, los registros de auditoría se conservarán, al menos, durante 15 años.

#### **5.4.4 Protección de los registros de auditoría**

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie, salvo las propias aplicaciones de visualización de eventos, con su debido control de accesos, pueda acceder a ellos.

Las copias de backup de dichos registros se almacenan en un archivo ignífugo cerrado dentro de las instalaciones seguras de la DGP

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorías de DNIe. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres Autoridades o del administrador del servicio auditado, y siempre que hayan transcurrido los 15 años de retención.

#### **5.4.5 Procedimientos de respaldo de los registros de auditoría**

Las copias de respaldo de los registros de auditoría se realizan según las medidas estándar establecidas por la DGP para las copias de respaldo de sus sistemas de información.

#### **5.4.6 Sistema de recogida de información de auditoría**

El sistema de recopilación de información de auditoría de la PKI es una combinación de procesos automáticos y manuales ejecutados por las aplicaciones de la PKI. Todos los registros de auditoría de las ACs, ARs, los registros del sistema operativo y los de red se almacenan en los sistemas internos de DNIE.

Todos los elementos significativos existentes en DNIE se acumulan en una Base de Datos. Los procedimientos de control de seguridad empleados en DNIE se basan en la tecnología de construcción empleada en la base de datos.

Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos, es decir, detecta una posible manipulación fraudulenta de los datos.
- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.
- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él. Esto permite guardar un registro de las operaciones realizadas y evita que se pierdan firmas electrónicas realizadas anteriormente por otros usuarios cuando se actualizan los datos.

La siguiente tabla es un resumen de los posibles peligros a los que una base de datos puede estar expuesta y que pueden detectarse con las pruebas de integridad:

- Inserción o alteración fraudulenta de un registro de sesión.
- Supresión fraudulenta de sesiones intermedias.
- Inserción, alteración o supresión fraudulenta de un registro histórico.
- Inserción, alteración o supresión fraudulenta del registro de una tabla de consultas.

#### **5.4.7 Notificación al sujeto causa del evento**

No se prevé la notificación automática de la acción de los ficheros de registro de auditoría al causante del evento.

#### **5.4.8 Análisis de vulnerabilidades**

El análisis de vulnerabilidades queda cubierto con el Plan de Auditoría de la DGP. Estos análisis son ejecutados semanal, mensual y anualmente

Los acontecimientos en el proceso de auditoría son guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad son ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados.

## **5.5 ARCHIVO DE REGISTROS**

### **5.5.1 Tipo de eventos archivados**

Cada Autoridad de Certificación definida en DNLe conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, manteniendo un registro de eventos.

Las operaciones registradas incluyen las realizadas por los administradores que utilizan las aplicaciones de administración de los elementos de DNLe, así como toda la información relacionada con el proceso de registro.

Los tipos de datos o ficheros que son archivados son, entre otros, los siguientes:

- Datos relacionados con el procedimiento de registro y solicitud de certificados
- Los especificados en el punto 5.4.1.
- El fichero histórico de claves.
- La Prácticas y Políticas de Certificación

### **5.5.2 Periodo de conservación de registros**

Toda la información y documentación relativa a los certificados se conservarán durante un mínimo de 15 años

Para los registros de auditoría se estará a lo especificado en el apartado 5.4.3, siempre atendiendo a cualquier particularidad especificada en la Política de Certificación del Certificado correspondiente a los datos involucrados.

### **5.5.3 Protección del archivo**

Los Archivos de registro están protegidos mediante técnicas criptográficas, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.

La destrucción de un archivo de Registro solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorías de DNLe. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres Autoridades o del administrador del servicio auditado, y siempre que haya transcurrido el periodo mínimo de retención (15 años).

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

Las copias de respaldo de los Archivos de registros se realizan según las medidas estándar establecidas por la DGP para las copias de respaldo del resto de sistemas de información de la DGP.

### **5.5.5 Requerimientos para el sellado de tiempo de los registros**

Los sistemas de información empleados por DNIE garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. Todos los servidores del sistema de DNIE están sincronizados en fecha y hora. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se autocalibran por distintos caminos, utilizando como referencia la del Real Instituto y Observatorio de la Armada

### **5.5.6 Sistema de archivo de información de auditoría .**

El sistema de recogida de información es interno a la DGP.

### **5.5.7 Procedimientos para obtener y verificar información archivada**

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Administrador de Auditoría que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la PKI.

## **5.6 CAMBIO DE CLAVES DE UNA AC**

Los procedimientos para proporcionar, en caso de cambio de claves de una AC, la nueva clave pública de AC a los titulares y terceros aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en el sitio web [www.dnielectronico.es](http://www.dnielectronico.es) y en el Boletín Oficial del Estado (ver apartado 2.1)

Los procedimientos para proporcionar una nueva clave pública a los usuarios de dicha AC corresponden al procedimiento de renovación recogido en este documento.

## **5.7 RECUPERACIÓN EN CASOS DE VULNERACIÓN DE UNA CLAVE Y DE DESATRE NATURAL U OTRO TIPO DE CATÁSTROFE**

### **5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades**

La DGP tiene establecido un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por DNLe.

El Plan de Contingencias contempla, entre otros aspectos, los siguientes:

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

En el caso de que se viera afectada la seguridad de los datos de verificación de firma de alguna Autoridad de Certificación, DNLe informará a todos los titulares de certificados de DNLe y terceros aceptantes conocidos que todos los certificados y listas de revocación firmados con estos datos ya no son válidos. Tan pronto como sea posible se procederá al restablecimiento del servicio.

### **5.7.2 Alteración de los recursos hardware, software y/o datos**

Si los recursos hardware, software, y/o datos se alteran o se sospecha que han sido alterados se detendrá el funcionamiento de la AC hasta que se reestablezca la seguridad del entorno con la incorporación de nuevos componentes cuya adecuación pueda acreditarse. De forma simultánea se realizará una auditoría para identificar la causa de la alteración y asegurar su no reproducción.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los usuarios de los mismos y se procederá a una nueva certificación.

### **5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una Autoridad**

En el caso de que se viera afectada la seguridad de la clave privada de una Autoridad se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente ARL, cesando el funcionamiento de actividad de la Autoridad.

En el caso de que la Autoridad afectada sea una AC, el certificado revocado de la misma permanecerá accesible en el repositorio de DNLe con objeto de continuar verificando los certificados emitidos durante su periodo de funcionamiento. La notificación de la revocación será hará efectiva a través del sitio web [www.dnielectronico.es](http://www.dnielectronico.es) y del Boletín Oficial del Estado (ver apartado 2.1)

Las Autoridades componentes de DNLe dependientes de la AC afectada serán informadas del hecho y conminadas a solicitar una nueva certificación por otra AC del dominio de certificación del DNLe.

Se notificará a todas las Autoridades afectadas que los certificados y la información sobre su revocación, suministrada con la clave comprometida de la AC, deja de ser válida desde el momento de la notificación.

Los certificados firmados por Autoridades dependientes de la AC afectada en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente, dejarán de ser validos por lo que sus titulares deberán solicitar la emisión de nuevos certificados.

#### **5.7.4 Instalación después de un desastre natural u otro tipo de catástrofe**

El sistema de PKI soporte del DNle se encuentra replicado en dos centros distantes en más de 70 km y que operan en modo espejo. No obstante, el sistema de Autoridades de Certificación de DNle puede ser reconstruido en caso de desastre (indisponibilidad continuada de ambos centros). Para llevar a cabo esta reconstrucción es necesario contar con:

- Un sistema con hardware, software y dispositivo Hardware Criptográfico de Seguridad similar al existente con anterioridad al desastre.
- Las tarjetas de administrador y oficial de seguridad de todas las Autoridades de Certificación de DNle.
- Las tarjetas de administrador y operador del HSM y backup del material criptográfico.
- Una copia de respaldo de los discos del sistema y de la BBDD anterior al desastre.

Con estos elementos es posible reconstruir el sistema tal y como estaba en el momento de la copia de respaldo realizada y, por lo tanto, recuperar la AC, incluidas sus claves privadas.

El almacenamiento, tanto de las tarjetas de acceso de los administradores de las ACs como de las copias de los discos de sistema de cada AC, se lleva a cabo en un lugar diferente, lo suficientemente alejado y protegido como para dificultar al máximo la concurrencia de catástrofes simultáneas en los sistemas en producción y en los elementos de recuperación.

### **5.8 CESE DE UNA AC O AR**

#### **5.8.1 Autoridad de Certificación**

En el caso de cesar la actividad de una de las AC, se adoptaran las medidas necesarias para que los potenciales problemas para los titulares de sus certificados y los terceros aceptantes sean los mínimos, así como el mantenimiento de los registros requeridos para proporcionar prueba cierta de la certificación a efectos legales.

En caso de cese de la actividad de una o de todas sus ACs, se comunicará a los titulares de sus certificados, a través del sitio web [www.dnielectronico.es](http://www.dnielectronico.es) y del Boletín Oficial del Estado y con un plazo mínimo de antelación de 2 meses al citado cese de actividad, su intención de que la/s AC correspondientes cesen en la actividad como prestadores de servicios de certificación.

En el supuesto de que la DGP decidiera transferir la actividad de Prestador de Servicios de Certificación a otro organismo, comunicará a los titulares de sus certificados los acuerdos de transferencia. A tal efecto DNIE enviará un documento explicativo de las condiciones de transferencia y de las características del Prestador al que se propone la transferencia de la gestión de los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y la recepción de la notificación, con una antelación mínima de 2 meses al cese efectivo de su actividad.

DNIE comunicará al Ministerio de Industria, Comercio y Turismo, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados especificando si va a transferir la gestión y a quién o si se extinguirá su vigencia.

Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad.

DNIE remitirá al Ministerio de Industria, Comercio y Turismo con carácter previo al cese definitivo de su actividad la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos previstos en el artículo 20.1.f de la Ley de Firma electrónica.

Transcurrido el plazo de dos meses, sin que exista acuerdo de transferencia los certificados serán revocados.

### **5.8.2 Autoridad de Registro**

No procede

## **6. CONTROLES DE SEGURIDAD TÉCNICA**

La infraestructura del DNLe utiliza sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

### **6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES**

#### **6.1.1 Generación del par de claves**

Los pares de claves para los componentes internos de la PKI del DNLe, concretamente AC Raíz y ACs Subordinadas, se generan en módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3 o superior nivel de seguridad. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

Las claves para los certificados de identidad y firma reconocida emitidos por la AC *Subordinada* se generan en la propia tarjeta criptográfica del titular, la cual cumple los requisitos de Dispositivo Seguro de Creación de Firma (nivel de seguridad CC EAL4+).

#### **6.1.2 Entrega de la clave privada al titular**

La clave privada se genera en presencia del titular en su tarjeta criptográfica y no es posible la extracción de la misma. No existe por tanto ninguna transferencia de clave privada.

#### **6.1.3 Entrega de la clave pública al emisor del certificado**

La clave pública se exporta de la tarjeta almacenada en un certificado Card Verificable, firmado por una clave de autenticación propia de la tarjeta. Este certificado Card Verificable es enviado a la PKI del DNLe formando parte de una de una solicitud de certificación en formato PKIX-CMP.

#### **6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes**

La clave pública de la AC Subordinada está incluida en el certificado de dicha AC.

El certificado de la AC Subordinada debe ser obtenido del repositorio especificado en este documento, donde queda a disposición de los titulares de certificados y terceros aceptantes para realizar cualquier tipo de comprobación.

El certificado de la AC raíz de la jerarquía del DNle, se publica también en el repositorio, en forma de certificado autofirmado. Se establecen medidas adicionales para confiar en el certificado autofirmado, como la comprobación de su huella digital que aparecerá publicada en el sitio web [www.dnielectronico.es](http://www.dnielectronico.es) y en el Boletín oficial del Estado.

### **6.1.5 Tamaño de las claves**

El tamaño de las claves de la AC Raíz es de 4096 bits.

El tamaño de las claves de las AC Subordinadas será de 2048

El tamaño de las claves de los certificados de identidad pública es de 2048 bits.

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

La clave pública de la AC Raíz y de la AC Subordinada está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA.

La clave pública de los certificados de identidad pública está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA.

La verificación de la calidad en ambos casos se realiza de acuerdo con el informe especial del ETSI SR 002 176, que indica la calidad de los algoritmos de firma electrónica. Los algoritmos y parámetros de firma utilizados por las Autoridades de Certificación del DNle para la firma de certificados electrónicos y listas de certificados revocados son los siguientes:

Algoritmo de firma: RSA

Parámetros del algoritmo de firma: Longitud del Módulo=4096/2048

Algoritmo de generación de claves: rsagen1

Método de relleno: emsa-pkcs1-v1\_5

Funciones criptográficas de Resumen: SHA-1/SHA-256

### **6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3)**

Los usos admitidos de la clave para cada tipo de certificado emitido por DNle vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por DNle contienen la extensión 'Key Usage' definida por el estándar X.509 v3, la cual se califica como crítica.

Ha de tenerse en cuenta que la eficacia de las limitaciones basadas en extensiones de los certificados depende, en ocasiones, de la operatividad de aplicaciones informáticas que no han sido fabricadas ni controladas por DNle.

La clave definida por la presente política, y por consiguiente el certificado asociado, se utilizará para la firma electrónica de correos electrónicos, ficheros y transacciones.

A tal efecto, en los campos 'Key Usage' de los certificados de Identidad Pública se han incluido los siguientes usos:

| CERTIFICADO  | KEY USAGE                      |
|--|--------------------------------|
| Certificado de Firma<br>(2.16.724.1.2.2.2.3)         | contentCommitment <sup>2</sup> |
| Certificado de Autenticación<br>(2.16.724.1.2.2.2.4) | Digital Signature              |

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

### 6.2.1 Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por AC Raíz y ACs *Subordinadas* de DNle cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3 o superior nivel de seguridad. Los sistemas de hardware y software que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2.

La puesta en marcha de cada una de las Autoridades de Certificación, teniendo en cuenta que se utiliza un módulo Criptográfico de seguridad (HSM), conlleva las siguientes tareas:

- a) Inicialización del estado del módulo HSM.
- b) Creación de las tarjetas de administración y de operador.
- c) Generación de las claves de la AC.

En cuanto a las tarjetas criptográficas con certificados para firma electrónica avanzada, aptas como dispositivos seguros de creación de firma, cumplen el nivel de seguridad CC EAL4+ y soportan los estándares PKCS#11 y CSP.

### 6.2.2 Control multipersona (k de n) de la clave privada

La clave privada, tanto de la AC Raíz como de AC *Subordinada*, se encuentra bajo control multipersona<sup>3</sup>. Ésta se activa mediante la inicialización del software de AC por medio de

---

<sup>2</sup> Nonrepudiation

una combinación de operadores de la AC, administradores del HSM y usuarios de S.O.. Éste es el único método de activación de dicha clave privada.

La clave privada de los Certificados de Identidad Pública está bajo el exclusivo control del ciudadano titular del DNI.

### **6.2.3 Custodia de la clave privada**

Las claves privadas de las Autoridades de Certificación que componen DNIE se encuentran alojadas en dispositivos criptográfico que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3 o superior nivel de seguridad.

La custodia de las claves privadas de los certificados de Identidad Pública la realizan los ciudadanos titulares de las mismas. En ningún caso la AC guarda copia de la clave privada ya que ésta no puede ser extraída de la tarjeta.

Las Claves Privadas del Ciudadano se encuentran almacenadas en el procesador de la tarjeta criptográfica del Documento Nacional de Identidad. Con esto se consigue que las Claves Privadas no abandonen nunca el soporte físico del DNI, minimizando las posibilidades de comprometer dichas claves.

Para el acceso a las claves y al certificado de firma el ciudadano deberá emplear una clave personal de acceso (PIN) generada en el momento de recibir su DNIE y que sólo él debe conocer.

En todo momento el ciudadano podrá modificar la clave personal de acceso en una Oficina de Expedición utilizando en los puestos destinados a tal efecto (Puntos de Actualización del DNIE) y mediante el siguiente procedimiento:

- Si conoce la clave personal de acceso – PIN - podrá emplearlo durante el proceso de cambio
- En caso de no recordar la clave personal de acceso – PIN - (o encontrase bloqueada la tarjeta al superar el número de intentos con un PIN incorrecto) podrá realizar el cambio mediante la comprobación de la biometría de impresión dactilar.

En ningún caso el olvido de la clave personal de acceso supondrá la revocación de los Certificados de Identidad Pública, siempre que pueda ser modificada por el procedimiento anterior.

También se habilitará un procedimiento telemático que permitirá el cambio de la clave personal de acceso – PIN - siempre que se recuerde el PIN vigente.

---

<sup>3</sup> Control multipersona: control por más de una persona, normalmente por un subconjunto 'k' de un total de 'n' personas. De esta forma, se garantiza que nadie tenga el control de forma individual de las actuaciones críticas a la vez que se facilita la disponibilidad de las personas necesarias.

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

Las claves privadas de las ACs del sistema del DNle están archivadas bajo la protección de los HSM que cada una de ellas posee y a los que sólo ellas y los administradores y operadores de la correspondiente AC tienen acceso. La clonación del material criptográfico de un HSM sólo es viable con la colaboración de un mínimo de tres administradores del HSM, operadores del HSM, un Administrador de Sistemas y los custodios del material criptográfico.

No es posible realizar una copia de seguridad de las claves privadas asociadas a los certificados de Identidad Pública (autenticación y firma electrónica) ya que las claves no pueden ser exportadas de las tarjetas y éstas no son clonables.

#### **6.2.5 Archivo de la clave privada**

Las claves privadas de la ACs del DNle pueden quedar (como copia de seguridad) almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes (de las que no pueden ser extraídas). Estas tarjetas son utilizadas para introducir la clave privada en el módulo criptográfico. Las copias de backup de las claves privadas se custodian en archivos seguros ignífugos.

Las claves privadas asociadas a los certificados de autenticación y firma electrónica de los ciudadanos titulares del DNle nunca son archivadas ya que no pueden ser exportadas de las tarjetas para garantizar el no repudio y el compromiso del ciudadano con el contenido de la firma.

#### **6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico**

La transferencia de la clave privada de las ACs del sistema del DNle sólo se puede hacer entre módulos criptográficos (HSM) y requiere de la intervención de un mínimo de tres administradores del HSM, operadores del HSM, un Administrador de Sistemas y los custodios del material criptográfico.

Las claves privadas asociadas a los certificados de Identidad y firma electrónica de los ciudadanos no pueden ser transferidas a o desde una tarjeta del DNle. La generación de claves y la importación de los certificados asociados sólo puede realizarse desde un puesto autorizado de una Oficina de Expedición

#### **6.2.7 Almacenamiento de la clave privada en un módulo criptográfico**

Las claves privadas se generan en el módulo criptográfico en el momento de la creación de cada una de las Autoridades de DNle que hacen uso de dichos módulos.

Las tarjetas soporte del DNle son dispositivos seguros de creación de firma y cumplen el nivel de seguridad CC EAL4+. Las claves privadas asociadas a la identidad del ciudadano se crean en la tarjeta criptográfica en presencia del mismo y en ningún caso es posible su extracción y/o exportación a otro dispositivo.

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

Tal y como se estipula en el apartado *6.2.2 Control multipersona de la clave privada*, la clave privada tanto de la AC Raíz como de la AC Subordinada, se activa mediante la inicialización del software de AC por medio de la combinación mínima de operadores de la AC correspondiente. Éste es el único método de activación de dicha clave privada.

La activación de las clave privadas y de los certificados de autenticación y firma requiere la introducción de la clave personal de acceso (PIN) del titular, clave que fue generada en el momento de la expedición del DNle y que debe permanecer bajo su exclusivo conocimiento.

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

Un Administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación del DNle mediante la detención del software de CA. Para su reactivación es necesaria la intervención mínima de los roles descritos en apartados anteriores.

Las claves privadas asociadas a los certificados de identidad Pública se pueden desactivar retirando la tarjeta del lector o pasado el tiempo establecido tras la introducción de la clave personal de acceso.

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

En términos generales la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.

En el caso de las ACs de la jerarquía del DNle la destrucción consistiría en el borrado seguro de las claves de los HSM que las albergase, así como de las copias de seguridad.

En el caso de los certificados de Identidad Pública del ciudadano, la destrucción de la clave privada:

- Se realizará en los procesos de renovación de dicha clave cuando no medie una renovación de la tarjeta de DNle asociada.
- Irá acompañada de la inutilización física de la tarjeta que la alberga, cuando se renueve el DNle (cada 5 o 10 años), cuando se deteriore la tarjeta de tal forma que no permita un uso eficiente de la misma o cuando se recupere un token perdido o sustraído.

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

### 6.3.1 Archivo de la clave pública

La Infraestructura de Clave Pública del DNLe, en cumplimiento de lo establecido por el artículo 20 f) de la LFE 59/2003 y en su vocación de permanencia mantendrá sus archivos por un periodo mínimo de treinta y cinco años (35) siempre y cuando la tecnología de cada momento lo permita.

### 6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves

Los periodos de utilización de las claves son los determinados por la duración del certificado, y una vez transcurrido no se pueden continuar utilizando.

El certificado y el par de claves de AC Raíz de DNLe tienen una validez de treinta (30) años y los de la AC Subordinada DNLe de quince (15) años.

La caducidad producirá automáticamente la invalidación de los Certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La caducidad de los Certificados de Identidad Pública ocurrirá 2 años y 6 meses a contar desde el día de su expedición a las 24:00 horas. En ningún caso la duración de los Certificados de Identidad Pública superarán a la fecha de caducidad impresa en el soporte plástico del DNI.

A partir de la fecha de caducidad de la tarjeta el ciudadano está obligado a renovar ambos elementos de identidad: el soporte plástico del DNI y los Certificados de Identidad Pública. No obstante, tal y como recoge el Real Decreto **1553/2005** la activación de los certificados tendrá carácter voluntario, por lo que el ciudadano podrá solicitar la revocación de los certificados emitidos como parte del proceso de expedición.

Los plazos de validez de la tarjeta DNI serán iguales a los actualmente establecidos: 5 y 10 años. La renovación de los Certificados sobre una misma tarjeta se deberá realizar, en la situación más habitual, 1 y 3 veces respectivamente. La renovación de los Certificados durante el periodo de validez de la tarjeta será voluntaria, y se emitirán de forma presencial guiada, sin la intervención de un funcionario (utilizando los Puntos de Actualización del DNLe habilitados a tal efecto en las Oficinas de Expedición) tras la correcta acreditación de la identidad del ciudadano.

En el caso que haya transcurrido más de 5 años desde la identificación inicial del ciudadano (es el caso de la segunda renovación de los certificados en soportes de 10 o más años), en cumplimiento del artículo 13 de la Ley de Firma Electrónica (*"La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará ..."*) la renovación a través de los Puntos de Actualización del DNLe requerirán la personación previa del ciudadano ante un funcionario de la Oficina de Expedición a los efectos del mencionado artículo.

La caducidad deja automáticamente sin validez a los Certificados contenidos en el DNle, originando el cese permanente de su operatividad conforme a los usos que le son propios.

La caducidad de un Certificado de Identidad Pública inhabilita el uso legítimo por parte del Ciudadano.

## **6.4 DATOS DE ACTIVACIÓN**

### **6.4.1 Generación e instalación de los datos de activación**

Para la instauración de una Autoridad de Certificación del dominio del DNle se deben crear tarjetas criptográficas, que servirán para actividades de funcionamiento y recuperación. La AC opera con varios tipos de roles, cada uno con sus correspondientes tarjetas criptográficas donde se almacenan los datos de activación.

Para la activación de las claves de las ACs es necesaria la intervención de los administradores del HSM que tienen capacidad para poner en estado operativo el HSM y de los usuarios del HSM que tienen el conocimiento del PIN o palabra de acceso del mismo que permite activar las claves privadas.

En el caso de las claves asociadas los certificados de autenticación y firma electrónica del ciudadano, el dato de activación consiste en la clave personal de acceso –PIN- de la tarjeta que las contiene. La habilitación de dicha clave personal se realiza en el momento de la inicialización de la misma, siendo generada por el sistema y entregada al ciudadano en forma de sobre ciego en el momento en que se generan las claves y permanece bajo su exclusivo conocimiento durante todo el ciclo de vida de las claves.

### **6.4.2 Protección de los datos de activación**

Sólo el personal autorizado, en este caso los Operadores y Administradores de la PKI del DNle correspondientes a cada AC, poseen las tarjetas criptográficas con capacidad de activación de las ACs y conoce las palabras de paso para acceder a los datos de activación.

En el caso de las claves asociadas a los certificados de Identidad Pública del ciudadano, sólo éste conoce la clave personal de acceso o PIN, siendo por tanto el único responsable de la protección de los datos de activación de sus claves privadas.

La clave personal de acceso (PIN) es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados en los servicios ofrecidos a través de una red de comunicaciones; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:

- Este PIN es confidencial, personal e intransferible

- Memorícelo y procure no anotarlo en ningún documento físico ni electrónico que conserve o transporte junto a su DNI
- No envíe ni comunique su PIN a nadie
- Si cree que su PIN puede ser conocido por otra persona, debe cambiarlo
- Usted podrá cambiar en cualquier momento su PIN personándose en las Oficinas del DNI o a través de INTERNET (en la dirección [www.dnielectronico.es](http://www.dnielectronico.es) en la que encontrará información adicional)
- Si usted cambia de PIN, se recomienda no escoger datos relacionados con su identidad personal (fecha de nacimiento, por ejemplo), ni con cualquier otro código que pueda resultar fácilmente perceptible por terceras personas (teléfono, series de números consecutivos, repeticiones de la misma cifra, secuencias de cifras que ya forman parte del número de su DNI, etc.)
- La introducción incorrecta de su PIN tres veces consecutivas, ocasionará el bloqueo de su tarjeta. Para resolver esta contingencia puede dirigirse a la Oficina de Expedición o al sitio web: [www.dnielectronico.es](http://www.dnielectronico.es)
- Se recomienda cambiarlo periódicamente.

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

En el caso de las claves asociadas a los certificados de Identidad Pública del ciudadano, éste podrá modificar de forma telemática los datos de activación (clave personal de acceso –PIN-) siempre que permanezcan bajo su conocimiento, esto es, no hayan sido olvidados o se haya bloqueado la tarjeta debido a intentos de acceso fallidos con datos de activación incorrectos.

En estos últimos casos, el ciudadano podrá modificar la clave personal de acceso –PIN- en los Puntos de Actualización del DNIe habilitados para tal efecto en las Oficinas de Expedición. El ciudadano podrá realizar el cambio de PIN o desbloqueo de la tarjeta haciendo uso de la biometría de sus impresiones dactilares.

## **6.5 CONTROLES DE SEGURIDAD INFORMÁTICA**

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos, como en el caso de auditorías externas o internas e inspecciones.

### **6.5.1 Requerimientos técnicos de seguridad específicos**

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

Asimismo, respecto de la gestión de la seguridad de la información, se sigue el esquema previsto en UNE-ISO 17799 *Código de Buenas Prácticas para la Seguridad de la Información*.

## **6.5.2 Evaluación de la seguridad informática**

Los procesos de gestión de la seguridad de la infraestructura soporte del DNIE son evaluados de forma permanente de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así como con la realización continua de controles de seguridad.

Las subsistemas que constituyen la PKI del DNIE son fiables, de acuerdo con la especificación técnica CEN CWA 14167-1, evaluándose el grado de cumplimiento mediante un perfil de protección adecuado, de acuerdo con la normativa EESSI y con la norma ISO 15408 o equivalente en el diseño, desarrollo, evaluación y adquisición de productos y sistemas de las Tecnologías de la Información, que vayan a formar parte del *sistema del DNIE*.

## **6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA**

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

### **6.6.1 Controles de desarrollo de sistemas**

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que puedan tener algún impacto sobre la seguridad de DNIE

Se realiza una análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizado en las aplicaciones de constituyen cada uno de sistemas del DNIE, para garantizar que los sistemas son seguros.

Se utilizan procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

La infraestructura del DNIE está dotada de entornos de desarrollo, preproducción y producción claramente diferenciados e independientes.

### **6.6.2 Controles de gestión de seguridad**

La organización encargada del sistema del DNIE, mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica y se realiza un seguimiento de las necesidades de capacidad.

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

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan algún impacto en la seguridad de DNIE.

## **6.7 CONTROLES DE SEGURIDAD DE LA RED**

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

No obstante indicar que, la infraestructura de la red utilizada por el sistema del DNIE está dotada de todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro (p.e. utilización de cortafuegos o intercambio de datos cifrados entre redes). Esta red también es auditada periódicamente.

## **6.8 FUENTES DE TIEMPO**

El Real Decreto 263/1996, que regula la utilización de técnicas y medios electrónicos, informáticos y telemáticos por la Administración General del Estado, modificado posteriormente por el Real Decreto 209/2003, establece que las comunicaciones y notificaciones realizadas a través de técnicas y medios electrónicos, informáticos y telemáticos serán válidas siempre que exista constancia de su fecha y hora, y en la Orden de Presidencia PRE/1551/2003 que lo desarrolla establece en su apartado séptimo *"La sincronización de la fecha y la hora de los servicios de registro telemático y de notificación telemática se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992 ..."*.

El Real Instituto y Observatorio de la Armada en San Fernando, a través de la Sección de Hora, tiene como misión principal el mantenimiento de la unidad básica de Tiempo, declarado a efectos legales como Patrón Nacional de dicha unidad, así como el mantenimiento y difusión oficial de la escala de "Tiempo Universal Coordinado", considerada a todos los efectos como la base de la hora legal en todo el territorio nacional, según el Real Decreto 1308/1992, de 23 de octubre.

Todos los sistemas que constituyen la infraestructura de clave pública del DNIE estarán sincronizados en fecha y hora utilizando como fuente segura de tiempos la proporcionada por el Real Instituto y Observatorio de la Armada.

## 7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

### 7.1 PERFIL DE CERTIFICADO

Los certificados de Identidad Pública emitidos por el sistema del DNIE serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la TS 101 862)

#### 7.1.1 Número de versión

Los certificados de identidad pública emitidos por la AC Subordinada utilizan el estándar X.509 versión 3 (X.509 v3)

#### 7.1.2 Extensiones del certificado

Los Certificados de Identidad Pública vinculan la identidad de una persona física (Nombre, Apellidos y número del Documento Nacional de Identidad) a una determinada clave pública, sin incluir ningún tipo de atributos al mismo. Para garantizar la autenticidad y no repudio en la Identidad Pública, toda esta información estará firmada electrónicamente por la Institución encargada de la emisión del DNIE

Los datos personales del Ciudadano incluidos en el Certificado son:

- Nombre y apellidos
- Número del Documento Nacional de Identidad
- Clave pública asociada al ciudadano
- Fecha de nacimiento, que podrá emplearse para comprobar la mayoría de edad del ciudadano, necesaria para firmar determinados documentos o acceder a ciertos servicios.

Las extensiones utilizadas en los certificados son:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- Auth. Information Access
- Biometricinfo

- Subject Directory Attributes
- qcstatements

DNIE tiene definida una política de asignación de OID's dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de DNIE comienzan con el prefijo 2.16.724.1.2.2.3.

DNIE tiene definidas las siguientes extensiones propietarias:

| OID                | Concepto         | Descripción  |
|--------------------|------------------|--|
| 2.16.724.1.2.2.3.1 | PersonalDataInfo | Hash de los datos biográficos (datos impresos en el DNI-e) |

A continuación se recogen los perfiles de los dos tipos de certificados que emite DNIE.

| Certificado de Firma de Ciudadano |   |                          |
|-----------------------------------|---|--------------------------|
| CAMPO                             | CONTENIDO   | CRÍTICA para extensiones |
| <b>Campos de X509v1</b>           |   |                          |
| 1. Versión                        | V3  |                          |
| 2. Serial Number                  | No secuencial   |                          |
| 3. Signature Algorithm            | SHA256withRSAEncryption<br>SHA1withRSAEncryption  |                          |
| 4. Issuer Distinguished Name      | CN=AC DNIE XXX <sup>4</sup><br>OU=DNIE<br>O=DIRECCION GENERAL DE LA POLICIA<br>C=ES                           |                          |
| 5. Validez                        | 30 meses  |                          |
| 6. Subject                        | CN=APELLIDO1 APELLIDO2, NOMBRE (FIRMA)<br>G=NOMBRE<br>SN=APELLIDO1<br>NÚMERO DE SERIE=DNI (con letra)<br>C=ES |                          |
| 7. Subject Public Key Info        | Algoritmo: RSA Encryption<br>Longitud clave: 2048 bits  |                          |
| <b>Campos de X509v2</b>           |   |                          |
| 1. issuerUniqueIdentifier         | No se utilizará   |                          |
| 2. subjectUniqueIdentifier        | No se utilizará   |                          |
| <b>Extensiones de X509v3</b>      |   |                          |
| 1. Subject Key Identifier         | Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.                              | NO                       |
| 2. Authority Key Identifier       | Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora.                        | NO                       |

<sup>4</sup> XXX es un número de tres dígitos que identifica a la AC emisora

| Certificado de Firma de Ciudadano                |  |                          |
|--|--|--------------------------|
| CAMPO  | CONTENIDO  | CRÍTICA para extensiones |
| <b>3. KeyUsage</b>                               |  | SI                       |
| Digital Signature                                | 0  |                          |
| ContentCommitment                                | 1  |                          |
| Key Encipherment                                 | 0  |                          |
| Data Encipherment                                | 0  |                          |
| Key Agreement                                    | 0  |                          |
| Key Certificate Signature                        | 0  |                          |
| CRL Signature                                    | 0  |                          |
| <b>4.extKeyUsage</b>                             | No se utilizará  |                          |
| <b>5. privateKeyUsagePeriod</b>                  | No se utilizará  |                          |
| <b>6. Certificate Policies</b>                   |  | NO                       |
| Policy Identifier                                | 2.16.724.1.2.2.2.3   |                          |
| URL DPC  | <a href="http://www.dnie.es/dpc">http://www.dnie.es/dpc</a>  |                          |
| Notice Reference                                 |  |                          |
| <b>7.Policy Mappings</b>                         |  |                          |
|  |  |                          |
| <b>8. Subject Alternate Names</b>                | No se utilizará  | NO                       |
| <b>9. Issuer Alternate Names</b>                 | No se utilizará  |                          |
| <b>10. Subject Directory Attributes</b>          | dateOfBirth  |                          |
| <b>11. Basic Constraints</b>                     |  | SI                       |
| Subject Type                                     | Entidad Final  |                          |
| Path Length Constraint                           | No se utilizará  |                          |
| <b>12. Policy Constraints</b>                    | No se utilizará  |                          |
| <b>13. CRLDistributionPoints</b>                 | No se utilizará  | NO                       |
| <b>14. Auth. Information Access</b>              | OCSP <a href="http://ocsp.dnie.es">http://ocsp.dnie.es</a><br>CA <a href="http://www.dnie.es/certs/ACraiz.crt">http://www.dnie.es/certs/ACraiz.crt</a> | NO                       |
| <b>15.netscapeCertType</b>                       | No se utilizará  |                          |
| <b>16. netscapeRevocationURL</b>                 | No procede   |                          |
| <b>17. netscapeCAPolicyURL</b>                   | No procede   |                          |
| <b>18. netscapeComment</b>                       | No procede   |                          |
| <b>19. Biometricinfo</b>                         | Hash de los datos biométricos SHA256/SHA1  | NO                       |
| <b>20. personalDataInfo (2.16.724.1.2.2.3.1)</b> | Hash de los datos biográficos (datos impresos en el DNIe) SHA1/SHA256  |                          |
| <b>21. qcstatements</b>                          | id-etsi-qcs-QcCompliance<br>id-etsi-qcs-QcSSCD   |                          |



| Certificado de Autenticación de Ciudadano |   |                          |
|---|---|--------------------------|
| CAMPO                                     | CONTENIDO   | CRÍTICA para extensiones |
| <b>Campos de X509v1</b>                   |   |                          |
| 1. Versión                                | V3  |                          |
| 2. Serial Number                          | No secuencial   |                          |
| 3. Signature Algorithm                    | SHA256withRSAEncryption<br>SHA1withRSAEncryption  |                          |
| 4. Issuer Distinguished Name              | CN=AC DNIE XXX<br>OU=DNIE<br>O=DIRECCION GENERAL DE LA POLICIA<br>C=ES  |                          |
| 5. Validez                                | 30 meses  |                          |
| 6. Subject                                | CN=APELLIDO1 APELLIDO2, NOMBRE (AUTENTICACIÓN)<br>G=NOMBRE<br>SN=APELLIDO1<br>NÚMERO DE SERIE=DNI (con letra)<br>C=ES |                          |
| 7. Subject Public Key Info                | Algoritmo: RSA Encryption<br>Longitud clave: 2048 bits  |                          |
| <b>Campos de X509v2</b>                   |   |                          |
| 1. issuerUniqueIdentifier                 | No se utilizará   |                          |
| 2. subjectUniqueIdentifier                | No se utilizará   |                          |
| <b>Extensiones de X509v3</b>              |   |                          |
| 1. Subject Key Identifier                 | Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.                                      | NO                       |
| 2. Authority Key Identifier               | Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora.                                | NO                       |
| 3. KeyUsage                               |   | SI                       |
| Digital Signature                         | 1   |                          |
| Content Commitment                        | 0   |                          |
| Key Encipherment                          | 0   |                          |
| Data Encipherment                         | 0   |                          |
| Key Agreement                             | 0   |                          |
| Key Certificate Signature                 | 0   |                          |
| CRL Signature                             | 0   |                          |
| 4. extKeyUsage                            | No se utilizará   |                          |
| 5. privateKeyUsagePeriod                  | No se utilizará   |                          |
| 6. Certificate Policies                   |   | NO                       |
| Policy Identifier                         | 2.16.724.1.2.2.2.4  |                          |
| URL DPC                                   | <a href="http://www.dnie.es/dpc">http://www.dnie.es/dpc</a>   |                          |

| Certificado de Autenticación de Ciudadano |  |                          |
|---|--|--------------------------|
| CAMPO                                     | CONTENIDO  | CRÍTICA para extensiones |
| Notice Reference                          |  |                          |
| 7. Policy Mappings                        |  |                          |
|   |  |                          |
| 8. Subject Alternate Names                | No se utilizará  | NO                       |
| 9. Issuer Alternate Names                 | No se utilizará  |                          |
| 10. Subject Directory Attributes          | dateOfBirth  |                          |
| 11. Basic Constraints                     |  | SI                       |
| Subject Type                              | Entidad Final  |                          |
| Path Length Constraint                    | No se utilizará  |                          |
| 12. Policy Constraints                    | No se utilizará  |                          |
| 13. CRLDistributionPoints                 | No se utilizará  | NO                       |
| 14. Auth. Information Access              | OCSP <a href="http://ocsp.dnie.es">http://ocsp.dnie.es</a><br>CA <a href="http://www.dnie.es/certs/ACraiz.crt">http://www.dnie.es/certs/ACraiz.crt</a> | NO                       |
| 15. netscapeCertType                      | No se utilizará  |                          |
| 16. netscapeRevocationURL                 | No procede   |                          |
| 17. netscapeCAPolicyURL                   | No procede   |                          |
| 18. netscapeComment                       | No procede   |                          |
| 19. BiometricInfo                         | Hash de los datos biométricos SHA256/SHA1  | NO                       |
| 20. personalDataInfo (2.16.724.1.2.2.3.1) | Hash de los datos biográficos (datos impresos en el DNI-e) SHA1/SHA256   |                          |
| 21. qcstatements                          | id-etsi-qcs-QcCompliance<br>id-etsi-qcs-QcSSCD   |                          |

Los certificados de Identidad Pública se emiten en calidad de certificados reconocidos y, por tanto ambos perfiles contienen los campos que establece la normativa legalmente aplicable en materia de Certificados Reconocidos:

**Artículo 11 del Capítulo II de la ley de firma 59/2003 de 19 Dic.**

**Anexo I de la Directiva del Parlamento Europeo 1999/93/EC**

| Requisitos Legales   | Modo de cumplimiento   |
|--|--|
| La indicación que se expiden como certificados reconocidos (artículo 11.2.a 59/2003) | Inclusión de la extensión Qualified Certificate Statements que incorpora las siguientes declaraciones: |

|   |   |
|---|---|
|   | <p>1.- id-etsi-qcs-QcCompliance – Indica que el certificado se emite como reconocido de acuerdo a los Anexo I y II de la Directiva del Parlamento Europeo 1999/93/EC y a la ley 59/2003, de 19 de diciembre, de firma electrónica.</p> <p>2.- id-etsi-qcs-QcSSCD –. Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo seguro de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/EC y a la ley 59/2003, de 19 de diciembre, de firma electrónica..</p>               |
| <p>La identificación del prestador de servicios de certificación que expide el certificado y el país en el que está establecido (artículo 11.2.c 59/2003)</p>   | <p>A través de la información que se recoge en el campo Issuer del certificado tal y como contempla la rfc 3739</p> <p>En el certificado se recoge claramente el país en el que se establece el PSC en el atributo Country del DN del campo Issuer</p> <p>En la presente DPC y en las Políticas de certificación asociadas, referenciadas en el certificado, se recoge el nombre o razón social, domicilio, dirección electrónica y número de identificación fiscal de la Institución que actúa como PSC del DNIe: Dirección General de la Policía.</p> |
| <p>La identificación del firmante (el suscriptor del certificado), por su nombre y apellidos y DNI o equivalente, o a través de un seudónimo que conste de manera inequívoca. (artículo 11.2.e 59/2003)</p> | <p>A través de la información que se recoge en el campo Subject del certificado tal y como contempla la rfc 3739: Nombre, Apellidos y DNI.</p> <p>No se contempla la utilización de seudónimos</p> <p>En el momento de elaboración de esta DPC y de las Políticas asociadas no se contempla la inclusión de la extensión Subject Alternative Names</p>  |
| <p>La inclusión de algún atributo del firmante (el suscriptor), relevante para el uso establecido para el certificado en la Política. (artículo 11.3 59/2003)</p>   | <p>Se utilizará la extensión Subject Directory Attributes para indicar la fecha de nacimiento como mecanismo para garantizar la capacidad para poder contratar y poder limitar el acceso a ciertos servicios</p> <p>[RFC3739] attributes: <i>dateOfBirth</i></p>  |
| <p>Los datos de verificación de firma que correspondan a los datos de creación de</p>   | <p>La clave pública del suscriptor se encuentra en el certificado tal y como</p>  |

|  |   |
|--|---|
| firma que se encuentren bajo el control del firmante. (artículo 11.2.f 59/2003)  | contempla la RFC 3280. (Subject Public Key Info)  |
| El comienzo y el final del periodo de validez del certificado. (artículo 11.2.g 59/2003)   | El periodo de validez de las claves y el certificado asociado se encuentra recogido en el campo del certificado contemplado en la ITU-T Recommendation X.509 y en RFC 3280  |
| El código identificativo único del certificado. (artículo 11.2.b 59/2003)  | La pareja formada por el Número de serie del certificado y el Issuer tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 3280   |
| La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado. (artículo 11.2.d 59/2003)       | La firma digital del emisor del certificado de acuerdo con la ITU-T Recommendation X.509 y la RFC 3280  |
| Los límites de uso del certificado, si se prevén. (artículo 11.2.h 59/2003)  | Estos límites estarán reflejados en la Políticas de Certificación asociadas a los certificados y en la extensión KeyUsage tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 3280.<br><br>Tal y como se ha indicado anteriormente se utilizará la extensión Subject Directory Attributes para indicar la fecha de nacimiento como mecanismo para garantizar la capacidad para poder contratar y para acceder a servicios con los certificados. |
| Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen. (artículo 11.2.i 59/2003) | No estipulado en el certificado   |

**Artículos 18,19,20 del Capítulo II de la ley de firma 59/2003 de 19 Dic.**

**Anexo II de la Directiva del Parlamento Europeo 1999/93/EC**

| <b>Requisitos Legales</b>   | <b>Modo de cumplimiento</b>  |
|---|--|
| El requisito B) establece la necesidad de un servicio de comprobación del estado de los certificados. (artículo 18.d 59/2003) | La extensión AIA (Authority Information Access) contiene la URL del servicio de validación de certificados de Identidad Pública.   |
| El requisito i) establece un periodo mínimo de retención de la información relevante (artículo 20.1.f 59/2003)                | No estipulado en el certificado<br><br>No se prevé la destrucción de la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación, aunque de establecer un periodo de retención, este no sería inferior a los 15 años establecidos en |

|  |  |
|--|--|
|  | la ley de Firma 59/2003  |
| El requisito K) establece que los términos y condiciones de uso de los certificados deben estar accesibles a las terceras partes que hacen uso del certificado. (artículo II.19.2 59/2003) | En la extensión CertificatePolicies se indica la URL en la que están accesibles esta DPC y las Políticas de Certificación asociada |

### 7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)

SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

### 7.1.4 Formatos de nombres

Los certificados emitidos por DNIe contienen el *distinguished name* X.500 del emisor y del titular del certificado en los campos *issuer name* y *subject name* respectivamente.

### 7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a 'Distinguished Names' X.500, que son únicos y no ambiguos.

El *DN* para los certificados de ciudadano estará compuesto de los siguientes elementos:

CN, GN, SN, SerialNumber, C

El atributo "C" (*countryName*) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en *PrintableString*.

Los atributos CN (Common Name), GN (Givenname), SN (Surname) y serialNumber del DN serán los que distinguan a los DN entre sí. La sintaxis de estos atributos es la siguiente:

CN= Apellido1 Apellido2, Nombre (AUTENTICACIÓN|FIRMA)

GN = Nombre

SN = Apellido1

SerialNumber= NNNNNNNNA (número de DNI con letra)

### 7.1.6 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente DPC es 2.16.724.1.2.2.2.1 Se le añade una extensión con formato X.Y que recoge la versión.

De esta forma el OID 2.16.724.1.2.2.2.1.X.Y correspondería a la release Y de la versión X de esta DPC

Los identificadores de las Políticas de Certificación asociadas bajo las que se emiten los certificados de Identidad Pública son los siguientes:

|   |   |
|---|---|
| Política de Certificados Reconocidos de Autenticación     | 2.16.724.1.2.2.2.4<br>(compatible con 0.4.0.1456.1.1) |
| Política de Certificados Reconocidos de Firma Electrónica | 2.16.724.1.2.2.2.3<br>(compatible con 0.4.0.1456.1.1) |

Como ocurre con la DPC al OID asignado a las Políticas de Certificación se le añadirá una extensión con formato X.Y para recoger la versión de las Políticas.

### 7.1.7 Uso de la extensión "PolicyConstraints"

No estipulado

### 7.1.8 Sintaxis y semántica de los "PolicyQualifier"

La extensión 'Certificate Policies' contiene los siguientes 'Policy Qualifiers':

- URL DPC: contiene la URL donde puede obtener la última versión de la DPC y de las Políticas de Certificación asociadas
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

No se tiene previsto incluir 'Notice Reference' en los certificados de Identidad Pública

### 7.1.9 Tratamiento semántico para la extensión "Certificate Policy"

Teniendo en cuenta los matices introducidos por la rfc3280 respecto al uso de esta extensión se decide Incluir el valor 2.5.29.32.0 en los certificados de las CAs (con lo que no se limitará para un futuro el conjunto de políticas que se podrán emitir bajo el dominio de certificación del DNIE). En los certificados de usuario de autenticación y firma se incluirían respectivamente los identificadores de política para autenticación (2.16.724.1.2.2.2.4) y firma (2.16.724.1.2.2.2.3) recogidos en esta DPC.

Por último la extensión está marcada en el documento como NO CRÍTICA para evitar problemas de interoperabilidad.

## 7.2 PERFIL DE CRL

### 7.2.1 Número de versión

La infraestructura del DNle soporta y utiliza CRLs X.509 versión 2 (v2)

### 7.2.2 CRL y extensiones

Las CRLs emitidas por el sistema del DNle serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework

## 7.3 PERFIL DE OCSP

### 7.3.1 Perfil del certificado OCSP responder

Los certificados de OCSP responder serán emitidos por una de las AC subordinadas del dominio de certificación del DNle y serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- IETF RFC 2560 Online Certificate Status Protocol – **OCSP**

El periodo de validez de los mismos será no superior a 6 meses. Tal y como contempla la rfc 2560, la AC emisora incluirá en el certificado de OCSP responder la extensión "*id-pkix-ocsp-nocheck*" para indicar que los clientes OCSP deben confiar en el prestador de servicios de validación durante el periodo de vida del certificado asociado. No obstante, la AC no descarta en un futuro incluir en la extensión AIA de los certificados de OCSP responder información acerca de mecanismos adicionales para comprobar la validez de dichos certificados.

### 7.3.2 Número de versión

Los certificados de OCSP Responder utilizarán el estándar X.509 versión 3 (X.509 v3)

### 7.3.3 Formatos de nombres

Los certificados de OCSP Responder emitidos por una AC del dominio del DNIE contendrán el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

Los nombres contenidos en los certificados están restringidos a 'Distinguished Names' X.500, que son únicos y no ambiguos.

El DN para los certificados estará compuesto de los siguientes elementos:

CN, OU, O, C

El atributo "C" (countryName) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en PrintableString, el resto de atributos se codificarán en UTF8:

CN= AV DNIE <ID PRESTADOR VALIDACION>

OU=<DATOS PRESTADOR VALIDACION>

OU=DNIE

O=DIRECCION GENERAL DE LA POLICIA

C=ES

### 7.3.4 Identificador de objeto (OID) de la Política de Certificación

El identificador de las Políticas de Certificación bajo la que se emiten los certificados de OCSP Responder del DNIE son los siguientes:

|  |                    |
|--|--------------------|
| Política de Certificados de OCSP Responder | 2.16.724.1.2.2.2.5 |
|--|--------------------|

Al OID asignado a las Política de Certificación se le añadirá una extensión con formato X.Y para recoger la versión de la Política.

### 7.3.5 Extensiones y Campos del certificado

Los campos y extensiones utilizadas en los certificados de OCSP Responder son:

version  
 serialNumber  
 subject  
 issuer  
 signingAlgorithms  
 validityPeriod  
 extKeyUsage  
 subjectKeyIdentifier  
 authorityKeyIdentifier issuerAndSerialPresent  
 KeyUsage. Calificada como crítica.  
 BasicConstraint. Calificada como crítica.  
 CertificatePolicies. Calificada como no crítica.  
 OCSPNocheck  
 AIA

A continuación se recogen el perfil del certificado de OCSP Responder que emite la infraestructura de clave pública del DNIE.

| Certificado de OCSP responder       |   |                          |
|-------------------------------------|---|--------------------------|
| CAMPO                               | CONTENIDO   | CRÍTICA para extensiones |
| <b>Campos de X509v1</b>             |   |                          |
| <b>1. Versión</b>                   | V3  |                          |
| <b>2. Serial Number</b>             | No secuencial   |                          |
| <b>3. Signature Algorithm</b>       | SHA256withRSAEncryption<br>SHA1withRSAEncryption <sup>5</sup>                       |                          |
| <b>4. Issuer Distinguished Name</b> | CN=AC DNIE XXX <sup>6</sup><br>OU=DNIE<br>O=DIRECCION GENERAL DE LA POLICIA<br>C=ES |                          |
| <b>5. Validez</b>                   | 6 meses   |                          |

<sup>5</sup> Inicialmente sha1 para garantizar la interoperabilidad de los clientes

<sup>6</sup> XXX es un número de tres dígitos que identifica a la AC emisora

| Certificado de OCSP responder |  |                          |
|-------------------------------|--|--------------------------|
| CAMPO                         | CONTENIDO  | CRÍTICA para extensiones |
| 6. Subject                    | CN= AV DNIE <ID PRESTADOR VALIDACION><br>OU=<DATOS PRESTADOR VALIDACION><br>OU=DNIE<br>O=DIRECCION GENERAL DE LA POLICIA<br>C=ES |                          |
| 7. Subject Public Key Info    | Algoritmo: RSA Encryption<br>Longitud clave: 2048 bits   |                          |
| <b>Campos de X509v2</b>       |  |                          |
| 1. issuerUniqueIdentifier     | No se utilizará  |                          |
| 2. subjectUniqueIdentifier    | No se utilizará  |                          |
| <b>Extensiones de X509v3</b>  |  |                          |
| 1. Subject Key Identifier     | Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.   | NO                       |
| 2. Authority Key Identifier   | Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora.   | NO                       |
| 3. KeyUsage                   |  | SI                       |
| Digital Signature             | 1  |                          |
| ContentCommitment             | 1  |                          |
| Key Encipherment              | 0  |                          |
| Data Encipherment             | 0  |                          |
| Key Agreement                 | 1  |                          |
| Key Certificate Signature     | 0  |                          |
| CRL Signature                 | 0  |                          |
| 4.extKeyUsage                 | OCSPSigning  |                          |
| 5. privateKeyUsagePeriod      | No se utilizará  |                          |
| 6. Certificate Policies       |  | NO                       |
| Policy Identifier             | 2.16.724.1.2.2.2.5   |                          |
| URL DPC                       | <a href="http://www.dnie.es/dpc">http://www.dnie.es/dpc</a>  |                          |
| Notice Reference              |  |                          |
| 7.Policy Mappings             | No se utilizará  |                          |
| 8. Subject Alternate Names    | No se utilizará  | NO                       |
| 9. Issuer Alternate Names     | No se utilizará  |                          |
| 10. Basic Constraints         |  | SI                       |
| Subject Type                  | Entidad Final  |                          |
| Path Length Constraint        | No se utilizará  |                          |
| 11. Policy Constraints        | No se utilizará  |                          |
| 12. CRLDistributionPoints     | No se utilizará  | NO                       |
| 13. Auth. Information Access  | CA <a href="http://www.dnie.es/certs/ACraiz.crt">http://www.dnie.es/certs/ACraiz.crt</a>   | NO                       |

| Certificado de OCSP responder |                                    |                          |
|-------------------------------|------------------------------------|--------------------------|
| CAMPO                         | CONTENIDO                          | CRÍTICA para extensiones |
| 14. OCSPNoCheck               | Valor NULL como contempla la norma | NO                       |

### 7.3.6 formato de las peticiones OCSP

Se deja al criterio del prestador del servicio de validación el soportar múltiples peticiones de validación en una única OCSPRequest tal y como contempla la rfc2560.

Se recomienda soportar la extensión Nonce (id-pkix-ocsp-nonce) tal y como contempla la norma para evitar "replay attacks".

### 7.3.7 formato de las respuestas

El OCSP responder de los prestadores de servicios de validación del DNIE deberá ser capaz, al menos, de generar respuestas de tipo id-pkix-ocsp-basic.

Respecto al estado de los certificados deberá responder como:

- "Revoked", para aquellos certificados emitidos por las AC del dominio de certificación del DNIE y que consten en las CRLs
- "Good", para aquellos certificados emitidos por las AC del dominio de certificación del DNIE y que no consten en las CRLs. El estado "good" es simplemente una respuesta "positiva" a la petición OCSP, indica que el certificado no está revocado pero no implica necesariamente que el certificado fue emitido alguna vez o que se encuentra dentro del periodo de validez.
- "unknown" si la petición corresponde a una AC emisora desconocida

Respecto a la semántica de los campos thisUpdate, nextupdate y producedAt.

- "producedAt" deberá contener el instante de tiempo en el que el OCSP responder genera y firma la respuesta
- "thisUpdate", debe indicar el momento en el que se sabe que el estado indicado en la respuesta es correcto. En el caso de certificados revocados deberá contener el campo "thisUpdate" de la CRL que se haya utilizado. En el resto de casos se utilizará la fecha local.
- "nextUpdate", debe indicar el instante de tiempo en el que se dispondrá de nueva información de revocación. En el caso de certificados revocados deberá contener el campo "nextUpdate" de la CRL que se ha utilizado, salvo cuando la fecha de "nextUpdate" sea anterior a la fecha local. En el resto de casos no se establecerá el campo nextUpdate, lo que es equivalente según rfc2560 a indicar que se puede disponer de nueva información de revocación en cualquier momento, con lo que es responsabilidad del cliente volver a consultar cuando lo estime oportuno

### **7.3.8 Fechado respuestas ocsp**

El prestador de servicios de validación deberá utilizar como fuente segura de tiempos la del *Real Instituto y Observatorio de la Armada* para habilitar los campos de fecha recogidos en el punto anterior.

## **8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES**

### **8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD**

Se llevará a cabo una auditoría interna sobre el sistema del DNle de forma anual, de acuerdo con el Plan de Auditorías de la DGP. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta DPC.

Sin perjuicio de lo anterior, que la DGP realizará auditorías internas bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

Entre las auditorías a realizar se incluye una auditoría bianual de cumplimiento de la legislación de protección de datos de carácter personal.

Igualmente cada tres años se llevará a cabo una auditoría externa para evaluar el grado de conformidad respecto a la especificación técnica ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates", teniendo en cuenta los criterios de la CWA 14172-2 ("EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes")

### **8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR**

La realización de las auditorías podrá ser encargada a empresas auditoras externas o al Departamento de Auditoría Interna en función de la disponibilidad de personal cualificado en los aspectos concretos a auditar y de lo que establezca el Plan de Auditorías.

Todo equipo o persona designada para realizar una auditoría de seguridad sobre el sistema DNle deberá cumplir los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la Institución de la que depende el sistema DNle.
- En general los criterios establecidos en la sección 3.4 de la CWA 14172-2 ("*Guidance on requirements for independent bodies, assessors, and assessment teams.*")

### **8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA**

Al margen de la función de auditoría, el auditor externo y la parte auditada (DNle) no deberán tener relación alguna que pueda derivar en un conflicto de intereses. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría.

### **8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES**

La auditoría determinará la adecuación de los servicios de DNle con esta DPC. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

En general los criterios establecidos en la sección 3.3 ("Introduction to conformity assessment of Certification Authorities") y 3.5 ("Guidance on the conformity assessment process") de la CWA 14172-2.

### **8.5 ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS**

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. La Autoridad de Aprobación de Políticas (AAP), en colaboración con el auditor, será la responsable de la determinación de las mismas.

En el caso de observarse deficiencias graves la Autoridad de Aprobación de Políticas podrá adoptar, entre otras, las siguientes decisiones: suspensión temporal de las operaciones hasta que las deficiencias se corrijan, revocación del certificado de la Autoridad, cambios en el personal implicado, invocación de la política de responsabilidades y auditorías globales más frecuentes.

### **8.6 COMUNICACIÓN DE RESULTADOS**

El equipo auditor comunicará los resultados de la auditoría a la Autoridad de Aprobación de Políticas de DNle (AAP), al Gestor de Seguridad del sistema del DNle, así como a los administradores de DNle y de la Autoridad en la que se detecten incidencias.

## **9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD**

### **9.1 TARIFAS**

#### **9.1.1 Tarifas de emisión de certificado o renovación**

No aplican.

La expedición del DNI está sometida al abono de la tasa, según la Ley 84/78, 28 de Diciembre que regula la tasa por expedición y renovación del DNI

Esta tasa es un tributo de carácter estatal que grava la expedición o renovación del Documento Nacional de Identidad.

Disposición final tercera del R.D 1553/2005. Tasas. El Gobierno promoverá la norma legal de rango adecuado para la adecuación de la tasa que haya de percibirse por la expedición del Documento Nacional de Identidad, de acuerdo con su coste y en consideración a los beneficios que proporciona a la comunidad.

Se renueva cada año mediante la Ley de Presupuestos Generales del Estado.

La última adecuación lo fue mediante la Ley 30/2005, de 29 de diciembre, fijando la cuantía en 6,60 euros y 11,90 euros para la tasa con recargo; a la entrada en vigor la presente DPC, la citada tasa no experimenta variación alguna como consecuencia de la emisión de los certificados electrónicos.

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

No aplica.

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

No aplica.

#### **9.1.4 Tarifas de otros servicios tales como información de políticas**

No se aplicará ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

### **9.1.5 Política de reembolso**

Al no existir ninguna tarifa de aplicación para esta Política de Certificación no es necesaria ninguna política de reintegros.

## **9.2 RESPONSABILIDADES ECONÓMICAS**

Subsumido en el apartado 9.8.

## **9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN**

### **9.3.1 Ámbito de la información confidencial**

Toda información que no sea considerada por DNLe como pública revestirá el carácter de confidencial. Se declara expresamente como información confidencial:

- Confidencialidad de la clave privada de la Autoridad de Certificación:

La Autoridad de Certificación garantiza la confidencialidad frente a terceros de su clave privada, la cual, al ser el punto de máxima confianza será generada y custodiada conforme a lo que se especifique en esta DPC.

- Confidencialidad de las claves de Identidad Pública del ciudadano:

Para garantizar la confidencialidad de las claves privadas, de autenticación y firma, del ciudadano, la Autoridad de Registro de la Institución del DNLe, proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro en presencia del ciudadano y de un funcionario de la Dirección General de la Policía y en un puesto que disponga de un dispositivo criptográfico específico. Dichas claves serán entregadas al ciudadano grabadas en el procesador de su DNLe basado en tarjeta criptográfica. Así mismo tanto la Autoridad de Registro como de Certificación no tendrán la posibilidad de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir estas claves ni para activarlas.

- Confidencialidad en la prestación de servicios de certificación:

La Institución del DNLe publicará exclusivamente los datos del ciudadano imprescindibles para el reconocimiento de su firma electrónica.

- Protección de datos

A efectos de lo dispuesto en la normativa sobre tratamiento de datos de carácter personal, se informa al ciudadano de la existencia de un fichero automatizado de datos de carácter personal creado y bajo la responsabilidad de la Dirección General de la Policía (Ministerio del Interior), con la finalidad de servir a los usos previstos en esta DPC o cualquier otro relacionado con los servicios de firma electrónica.

El Responsable del fichero se compromete a poner los medios a su alcance para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal contenidos en el fichero. Asimismo, se informa sobre el derecho que asiste al ciudadano para acceder o rectificar sus datos de carácter personal, siempre que se aporte la documentación necesaria para ello.

- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación Vinculada y sus auditores.
- Planes de continuidad de negocio y de emergencia. Política y planes de seguridad
- La información de negocio suministrada por sus proveedores y otras personas con las que la Institución del DNIE tiene el deber de guardar secreto establecida legal o convencionalmente.
- Toda la información clasificada como “Confidencial”

### **9.3.2 Información no confidencial**

Se considera información pública y por lo tanto accesible por terceros:

- La contenida en la presente Declaración de Prácticas y Políticas de Certificación.
- La información sobre el estado de los certificados.
- Toda otra información identificada como “Pública”

### **9.3.3 Deber de secreto profesional**

Los miembros de la Institución del DNIE que participen en cualesquiera tareas propias o derivadas de la DNIE están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable.

Asimismo el personal contratado que participe en cualquier actividad u operación del DNIE estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con la Institución del DNIE.

## **9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL**

### **9.4.1 Política de protección de datos de carácter personal**

De acuerdo con la legislación española al respecto, se recoge dentro del capítulo 10, apartado 10.1 y siguientes.

### **9.4.2 Información tratada como privada**

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal.

De conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados en todo caso como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación
- Toda otra información identificada como "Información privada"

En cualquier caso, los datos captados por el prestador de servicios de certificación tendrán la consideración legal de datos de nivel alto.

La información confidencial de acuerdo con la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

#### **9.4.3 Información no calificada como privada**

Es considerada no confidencial la siguiente información:

- Los certificados
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados, así como el resto de informaciones de estado de revocación.

#### **9.4.4 Responsabilidad de la protección de los datos de carácter personal**

Esta responsabilidad se regula en el capítulo 10.

#### **9.4.5 Comunicación y consentimiento para usar datos de carácter personal**

Se llevará a cabo en el procedimiento de primera inscripción, informando a los suscriptores de la obtención de sus datos personales

#### **9.4.6 Revelación en el marco de un proceso judicial**

Los datos de carácter personal solo podrán ser comunicados a terceros, sin consentimiento del afectado, en los supuestos contemplados en la legislación reguladora de protección de datos de carácter personal.

#### **9.4.7 Otras circunstancias de publicación de información**

Estas posibles circunstancias se regulan en el capítulo 10.

### **9.5 DERECHOS DE PROPIEDAD INTELECTUAL**

En los términos establecidos en el Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, la Dirección General de la Policía (Ministerio del Interior) es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta DPC. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la Dirección General de la Policía (Ministerio del Interior) sin la autorización expresa por su parte.

En el momento de elaborar esta versión de documento, la DGP tiene asignado el OID **2.16.724.1.2** perteneciente a la rama de OID *Country assignments* de *ISO-ITU-T* (también tiene asignado el OID 1.3.6.1.4.1.11537 perteneciente a la rama *Private Enterprise* de OID de IANA). Para el DNle se utilizará el OID asignado por ISO-ITU-T.

Queda prohibido, salvo acuerdo expreso con la Dirección General de la Policía, el uso total o parcial de cualquiera de los OID asignados a la DGP salvo para los usos específicos con que se incluyeron en el Certificado o en el Directorio.

### **9.6 OBLIGACIONES**

#### **9.6.1 Obligaciones de la AC**

La Autoridad de Certificación *Subordinada* de DNle actuará relacionando una determinada clave pública con su titular a través de la emisión de un certificado de firma reconocida, todo ello de conformidad con los términos de esta DPC.

Los servicios prestados por la AC en el contexto de esta DPC son los servicios de emisión, renovación y revocación de certificados de firma reconocida personales y la provisión del dispositivo seguro de creación de firma..

La AC tiene las siguientes obligaciones:

- 1º Realizar sus operaciones en conformidad con esta DPC.
- 2º Publicar esta DPC en el sitio web referido en el apartado *2.1 Repositorio*.
- 3º Comunicar los cambios de esta DPC de acuerdo con lo establecido en el apartado *9.12.2 Periodo y mecanismo de Notificación*
- 4º Cursar en línea la solicitud de un certificado y minimizar el tiempo necesario para expedir dicho certificado.
- 5º Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- 6º Revocar los certificados en los términos de la sección *4.4 Suspensión y Revocación de Certificados* y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web referidos en el apartado *2.1 Repositorio*, con la frecuencia estipulada en el punto *4.9.7 Frecuencia de emisión de CRLs*
- 7º En el caso que la AC proceda de oficio a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con esta DPC
- 8º Actualizar en línea y publicar las bases de datos de certificados en vigor y certificados revocados.
- 9º Poner a disposición de los ciudadanos los certificados correspondientes a la(s) Autoridad(es) de Certificación de la Dirección General de la Policía (Ministerio del Interior).
- 10º Proteger la clave privada de la(s) Autoridad(es) de Certificación de la Dirección General de la Policía (Ministerio del Interior).
- 11º Conservar registrada toda la información y documentación relativa a los certificados de identidad pública durante un mínimo de quince años.
- 12º Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte
- 13º No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados de identidad pública.
- 14º Colaborar con los procesos de auditoría.
- 15º Operar de acuerdo con la legislación aplicable. En concreto con:
  - La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
  - La Ley 59/2003, de 19 de diciembre, de Firma Electrónica
  - La L. O. 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal
- 16º En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ellas emitidos y al Ministerio de Industria, Comercio y Turismo tal como se recoge en el epígrafe 5.8.1.

### **9.6.2 Obligaciones de la AR**

Las Oficinas de Expedición del DNIe en su función de AR deberán cumplir las siguientes obligaciones:

- 1º Realizar sus operaciones en conformidad con esta DPC
- 2º Comprobar exhaustivamente la identidad de las personas
- 3º Notificación de la emisión de la pareja de certificados al ciudadano. No almacenando ni copiando los datos de creación de firma.
- 4º Tramitar las peticiones de revocación lo antes posible.
- 5º Notificación al ciudadano de la revocación o suspensión de sus certificados cuando se produzca de oficio por la Dirección General de la Policía (Ministerio del Interior), o a petición de la Autoridad competente.
- 6º Comprobar que toda la información incluida o incorporada por referencia en el certificado es exacta así como el resto de los datos que se graben en el procesador de la tarjeta criptográfica del Documento Nacional de Identidad.
- 7º Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado 10.
- 8º Poner a disposición de los ciudadanos, en las oficinas de expedición del DNI, los mecanismos adecuados para que pueda comprobar la veracidad de los datos contenidos en el procesador de la tarjeta criptográfica del Documento Nacional de Identidad.

### **9.6.3 Obligaciones de los ciudadanos titulares de los certificados**

Es obligación de los titulares de los certificados emitidos bajo la presente DPC:

- 1º Suministrar a las Autoridades de Registro información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.
- 2º Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta DPC que le sean de aplicación, así como las modificaciones que se realicen sobre las mismas.
- 3º Conservar y utilizar de forma correcta el Documento Nacional de Identidad y los Certificados y claves. Su titular estará obligado a la custodia y conservación del mismo.
- 4º Comunicar a la Dirección General de la Policía, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento de la tarjeta.
- 5º Proteger sus claves privadas y custodiar los Certificados asociados, tomando las precauciones razonables para evitar su pérdida, revelación, alteración o uso no autorizado.
- 6º Aceptar las restricciones de uso (apartado 1.4.2) impuestas a sus claves y certificados emitidos por la Dirección General de la Policía (Ministerio del Interior).

- 7º Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros de la clave personal de acceso y detección de inexactitudes en la información. La forma en que puede realizarse esta solicitud se encuentra especificada en el apartado 4.9.3.
- 8º No revelar la clave personal de acceso que permite la utilización de los certificados de identidad pública.
- 9º Informar inmediatamente a la Dirección General de la Policía (Ministerio del Interior) acerca de cualquier situación que pueda afectar a la validez del Certificado.
- 10º Asegurarse de que toda la información contenida en el Certificado y en el Documento Nacional de Identidad es correcta. Notificarlo inmediatamente en caso contrario.
- 11º No monitorizar, manipular o realizar actos de “ingeniería inversa” sobre la implantación técnica (hardware y software) de los servicios de certificación, sin permiso previo por escrito de la Autoridad de Certificación.
- 12º Cumplir las obligaciones que se establecen para el suscriptor en este documento y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

#### **9.6.4 Obligaciones de los terceros aceptantes**

A) Es obligación de los terceros que acepten y confíen en los certificados emitidos por DNIe:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y en esta DPC.
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o ha sido o revocado.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez, revocación e los certificados en que confía.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo, utilizando los medios que la DGP publique en el sitio Web [www.dnielectronico.es](http://www.dnielectronico.es)

B) Los prestadores de servicios telemáticos deberán verificar la validez de las firmas generadas por los ciudadanos a través de la red de Prestadores de Servicios de Validación

- En el supuesto que no se realice dicha comprobación, la Dirección General de la Policía (Ministerio del Interior) no se hace responsable del uso y confianza que los prestadores de servicios telemáticos otorguen a dichos certificados.
- En caso que el Prestador de Servicios Telemáticos consulte en línea el estado de un Certificado de Identidad Pública (bien de autenticación o bien de firma) debe almacenar el comprobante de la transacción para tener derecho a realizar posteriores reclamaciones en caso que el estado del certificado en el momento de la consulta no coincida con su situación real.

C) Confianza en las firmas:

- El prestador de servicios telemáticos debe adoptar las medidas necesarias para determinar la fiabilidad de la firma, construyendo toda la cadena de certificación y verificando la caducidad y el estado todos los certificados en dicha cadena.
- El prestador de servicios telemáticos debe conocer e informarse sobre las Políticas y Prácticas de Certificación emitidos por la Dirección General de la Policía (Ministerio del Interior).
- Cuando se realice una operación que pueda ser considerada ilícita o se de un uso no conforme a lo establecido en esta DPC, no se deberá confiar en la firma emitida por el certificado

D) Para confiar en los Certificados emitidos por la Dirección General de la Policía (Ministerio del Interior), el prestador de servicios telemáticos deberá conocer y aceptar toda restricción a que esté sujeto el citado Certificado.

### **9.6.5 Obligaciones de otros participantes**

No estipulado

## **9.7 LIMITACIONES DE RESPONSABILIDAD**

Subsumido en 9.8.

## **9.8 RESPONSABILIDADES**

### **9.8.1 Limitaciones de responsabilidades**

La DGP como Órgano que tiene atribuidas las competencias del DNle responderá en el caso de incumplimiento de las obligaciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y normativa de desarrollo, y en la presente DPC

### **9.8.2 Responsabilidades de la Autoridad de Certificación**

- La Dirección General de la Policía (Ministerio del Interior) responderá por los daños y perjuicios que causen a cualquier ciudadano en el ejercicio de su actividad

cuando incumpla las obligaciones que les impone la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extra-contractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.
- De manera particular, la DGP como prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.
- La DGP como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.
- La Dirección General de la Policía (Ministerio del Interior) no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del ciudadano y/o del prestador de servicio telemáticos.
- La Dirección General de la Policía (Ministerio del Interior) no será responsable de la utilización incorrecta de los Certificados ni las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información almacenada en el procesador de la tarjeta criptográfica del Documento Nacional de Identidad.
- La Dirección General de la Policía (Ministerio del Interior) no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del Certificado.
- La Dirección General de la Policía (Ministerio del Interior) no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta DPC si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.
- La Dirección General de la Policía (Ministerio del Interior) no será responsable del contenido de aquellos documentos firmados electrónicamente por los ciudadanos con el Certificado de Identidad Pública contenido en el DNI.
- La Dirección General de la Policía no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta DPC y en la Ley.

### **9.8.3 Responsabilidades de la Autoridad de Registro**

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los ciudadanos y la validación de sus datos, con las mismas limitaciones que se establecen en el apartado anterior para la Autoridad de Certificación.

### 9.8.4 Responsabilidades del ciudadano

El ciudadano asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

Así mismo el ciudadano se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios telemáticos. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios telemáticos deberán ser proporcionados por éste al ciudadano.

El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y es responsable de la conservación del mismo.

### 9.8.5 Delimitación de responsabilidades

Las ACs de DNIE no asumen ninguna responsabilidad en caso de pérdida o perjuicio:

|        |  |
|--------|--|
| RESP.1 | De los servicios que prestan, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible. |
| RESP.2 | Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario  |
| RESP.3 | Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL   |
| RESP.3 | Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta DPC.  |
| RESP.4 | Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por DNIE  |
| RESP.5 | Ocasionados por el mal uso de la información contenida en el certificado.  |
| RESP.6 | La AC no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se autenticquen mediante un certificado emitido por ella.  |

### 9.8.6 Alcance de la cobertura

De acuerdo con el artículo 16.1 de la Ley 59/2003 de Firma Electrónica, la DGP como Órgano competente de la Infraestructura de Clave Pública del DNIE está exento de la constitución de garantía la que se refiere el apartado 2 del artículo 20 de la mencionada ley:

**“Artículo 16. Requisitos y características del documento nacional de identidad electrónico** 1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan

*certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20...”*

### **9.8.7 Cobertura de seguro u otras garantías para los terceros aceptantes**

De acuerdo con el artículo 16.1 de la Ley 59/2003 de Firma Electrónica, la DGP (Ministerio Interior) está exenta de la constitución de garantía la que se refiere el apartado 2 del artículo 20 de la mencionada ley. Sin embargo se estará a lo dispuesto por la ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común

## **9.9 LIMITACIONES DE PÉRDIDAS**

A excepción de lo establecido por las disposiciones de la presente DPC, la DGP no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

## **9.10 PERIODO DE VALIDEZ**

### **9.10.1 Plazo**

Esta DPC entra en vigor desde el momento de su publicación en BOE y en el repositorio de DNIE.

Esta DPC estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC Raíz, momento en que obligatoriamente se dictará una nueva versión.

### **9.10.2 Sustitución y derogación de la DPC**

Esta DPC será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la DPC quede derogada se retirará del repositorio público de DNIE, si bien se conservará durante 15 años.

### **9.10.3 Efectos de la finalización**

Las obligaciones y restricciones que establece esta DPC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de DNIe, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

## **9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES**

Sin perjuicio de lo establecido en el apartado 4º de esta DPC, sobre requisitos operacionales para el ciclo de vida de los certificados, los titulares del DNI electrónico podrán comunicarse con la Dirección General de la Policía como entidad que tiene atribuidas las competencias de la infraestructura de clave pública, mediante mensaje electrónico o por escrito mediante correo postal dirigido a cualquiera de las direcciones contenidas en el punto *1.5 Administración de las Políticas*.

En el sitio web [www.dnielectronico.es](http://www.dnielectronico.es) estarán disponibles otros mecanismos de contacto con la entidad competente.

Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

## **9.12 PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES**

### **9.12.1 Procedimiento para los cambios**

La Autoridad con atribuciones para realizar y aprobar cambios sobre esta DPC es la Autoridad de Aprobación de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado *1.5 Administración de las Políticas* de esta DPC.

### **9.12.2 Periodo y procedimiento de notificación**

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se comunicará a los usuarios de los certificados correspondientes que se ha efectuado un cambio y que deben consultar la nueva DPC en el repositorio establecido. El mecanismo de comunicación será la dirección de Internet <http://www.dnielectronico.es> y el Boletín Oficial del Estado.

### **9.12.3 Circunstancias en las que el OID debe ser cambiado**

En los casos en que, a juicio de la AAP, los cambios de las especificaciones no afecten a la aceptabilidad de los certificados se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el

resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados.

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los usuarios de los certificados según lo establecido en el punto 9.12.2.

### **9.13 RECLAMACIONES Y JURISDICCIÓN**

Todas reclamaciones entre usuarios y DNle deberán ser comunicadas por la parte en disputa a la Autoridad de Aprobación de Políticas (AAP) de la DGP, con el fin de intentar resolverlo entre las mismas partes.

Para la resolución de cualquier conflicto que pudiera surgir con relación a esta DPC, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la Jurisdicción Contencioso Administrativa

[Los conflictos](#)

### **9.14 NORMATIVA APLICABLE**

Las operaciones y funcionamiento de DNle, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica
- Ley 84/78, 28 de Diciembre que regula la tasa por expedición y renovación del DNI

### **9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE**

Es responsabilidad de la Autoridad de Aprobación de Políticas velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

## **9.16 ESTIPULACIONES DIVERSAS**

### **9.16.1 Cláusula de aceptación completa**

Todos los Terceros Aceptantes asumen en su totalidad el contenido de la última versión de esta DPC.

### **9.16.2 Independencia**

En el caso de que una o más estipulaciones de esta DPC sea o llegase a ser inválida, nula, o inexigible legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la DPC careciera ésta de toda eficacia jurídica.

### **9.16.3 Resolución por la vía judicial**

No estipulado

## **9.17 OTRAS ESTIPULACIONES**

No se contemplan.

## **10. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

### **10.1 RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS**

Es competencia del Ministerio del Interior el ejercicio de las funciones relativas a la gestión, dirección, organización, desarrollo y administración de todos aquellos aspectos referentes a la expedición y confección del Documento Nacional de Identidad, conforme a lo previsto en la legislación en materia de seguridad ciudadana y de firma electrónica.

Corresponde, por tanto, a la DGP la gestión, administración, tratamiento, uso y custodia de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad. A tal efecto, la Orden INT/1751/2002, de 20 de junio, por la que se regulan los ficheros informáticos de la Dirección General de la Policía, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispone la aprobación de la creación del fichero ADDNIFIL, cuya finalidad es la gestión del Documento Nacional de Identidad, y su sometimiento al ámbito de aplicación de dicha ley y al régimen general de la misma, constatando que su titularidad corresponde a la Dirección General de la Policía, siéndole igualmente de aplicación el Real Decreto 994/1999, de 11 de junio, relativo a las medidas de seguridad exigibles y que han de ser recogidas en el preceptivo Documento de Seguridad.

No obstante, DNIe pone a disposición de los prestadores de servicios de validación las listas de certificados revocados para el cumplimiento diligente de los servicios de certificación.

El prestador de servicios de validación tendrá en todo caso la condición de encargados del tratamiento, sometiendo su actividad a lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. De este modo, el prestador de servicios de validación como cesionario de esta información únicamente podrá utilizar los datos que le sean facilitados de acuerdo con esas finalidades. Igualmente, todas las entidades que actúen como prestadores de servicios de certificación deberán a su vez adoptar su correspondiente documento de seguridad, tal y como exige para el encargado del tratamiento el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

Se facilitará al interesado el ejercicio de los derechos de oposición, acceso, rectificación y cancelación de sus datos de carácter personal, en los términos y plazos legales.

### **10.2 CREACIÓN DEL FICHERO E INSCRIPCIÓN REGISTRAL**

Los datos de creación e inscripción del fichero ADDNIFIL de la Dirección General de la Policía son:

- Creación: Orden INT/1751/2002, de 20 de junio
- Publicación: BOLETÍN OFICIAL DEL ESTADO N° 165, de 11 de julio de 2002
- N° de inscripción en el Registro General de Protección de Datos: 2022840185

Asimismo, el nombre del fichero, su responsable y el área encargada de atender las peticiones de ejercicio de derechos son:

|                                  |   |
|----------------------------------|---|
| Nombre del Fichero:              | ADDNIFIL  |
| Responsable del Fichero:         | Ministerio del Interior<br>Dirección General de la Policía<br>Comisaría General de Extranjería y Documentación    |
| Servicio de Atención al Público: | Secretaría General de la Comisaría General de Extranjería y Documentación<br>C/ General Pardiñas, 90 28071 Madrid |

## 10.3 DOCUMENTO DE SEGURIDAD LOPD

### 10.3.1 Aspectos cubiertos

La presente DPC, tal como se señala en el punto 1.1, se ha hecho de acuerdo a la especificación RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"* del Internet Engineering Task Force (IETF) para este tipo de documentos.

No obstante lo expuesto en los apartados 5 *"Controles de seguridad física, instalaciones, gestión y operacionales"* y 8 *"Auditorías de cumplimiento y otros controles"* de esta DPC y teniendo en cuenta lo dispuesto en el artículo 19.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que considera la DPC como documento de seguridad, a los efectos previstos en la legislación en materia de protección de datos de carácter personal, resulta obligado añadir el presente apartado con objeto de recoger todos los requisitos contemplados en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados con Datos de Carácter Personal

A tal fin se tratan los siguientes aspectos:

- Estructura básica de datos de carácter personal.
- Nivel de seguridad aplicable.
- Sistemas de Información que soportan el fichero
- Relación de usuarios
- Notificación y Gestión de Incidencias
- Copias de respaldo y recuperación
- Control de Accesos
- Ficheros Temporales
- Gestión de Soportes
- Utilización de datos reales en pruebas

El resto de aspectos que debe recoger un Documento de Seguridad han sido ya incluidos en capítulos anteriores de la presente DPC.

El objeto del Documento de Seguridad es preservar los datos de carácter personal procesados por el sistema del DNLe, por lo que afecta a todos aquellos recursos (personas, equipos, comunicaciones, software, procedimientos) implicados en el tratamiento de los datos.

### 10.3.2 Funciones y obligaciones del personal

Esta DPC, así como futuras versiones de la misma, son conocidas por todas las personas que acceden a los datos de carácter personal gestionados por DNLe, siendo de obligado cumplimiento todas las funciones y obligaciones que establece.

El apartado 5.3 recoge los controles de personal establecidos en la gestión de la infraestructura de clave pública del DNLe.

### 10.3.3 Estructura de datos de carácter personal

En la siguiente tabla se recogen los datos, utilizando las denominaciones utilizadas en el formulario de notificación de ficheros a la Agencia Española de Protección de Datos, de los titulares de certificados tratados por DNLe:

| <b>DATOS TRATADOS</b>                      |
|--|
| <b>Datos de carácter identificativo</b>    |
| <b>FILIACIÓN</b>                           |
| Nombre y apellidos                         |
| Fecha y Lugar de Nacimiento                |
| Nombre de los Padres                       |
| Sexo                                       |
| <b>Datos de características personales</b> |
| Número del DNI                             |
| Domicilio                                  |
| Teléfono                                   |
| Fotografía                                 |
| Firma                                      |
| Impresiones dactilares                     |
| Número de serie certificado electrónico    |

En el apartado 7 se recoge la estructura detallada del perfil del certificado.

#### 10.3.4 Nivel de seguridad

Aún cuando la naturaleza de los datos de carácter personal tratados exige la implantación de medidas de seguridad de nivel básico, dadas las especiales características de seguridad que ha de tener la PKI del DNIe y el nivel de seguridad que establece esta DPC, se implantarán medidas de seguridad de nivel alto.

#### 10.3.5 Sistemas de información

Dentro de la estructura de sistemas de información que constituye la PKI DNIe se pueden distinguir tres subsistemas con alguna implicación en el tratamiento de datos de carácter personal. A continuación se relacionan y describen de forma sintética:

- **Subsistema de gestión de certificados:** Se encarga de la creación de los certificados conforme al estándar X.509v3, donde se introducen las claves generadas por el subsistema de generación de claves y otros datos identificativos que se definen en esta DPC.
- **Subsistema de Autoridad de Registro:** Se encarga de la identificación del solicitante del certificado para proceder a la emisión posterior del certificado por DNIe.
- **Subsistema de publicación:** Se encarga de la gestión de la publicación de las Listas de Revocados (CRL) y del Directorio de certificados.

#### 10.3.6 Relación de usuarios

El Coordinador de Seguridad mantiene una relación de los usuarios con acceso a los datos de carácter personal tratados por la PKI en la que se indica su rol y nivel de acceso. Dicha relación de usuarios tiene carácter confidencial por motivos de seguridad, por lo que será precisa una petición motivada al Coordinador de Seguridad para tener acceso a la misma.

No se incluyen en esa relación los usuarios con acceso a los certificados electrónicos a efectos de hacer uso de los mismos para el envío de información cifrada ni los usuarios con acceso a las CRL.

#### 10.3.7 Notificación y gestión de incidencias

Los procedimientos internos del Departamento de Sistemas de Información asociados a la gestión de problemas aseguran que todas las incidencias se registran y documentan, realizándose un seguimiento de las mismas. Se registra información relativa a: fecha, hora, tipo de incidencia, persona que comunica la misma, persona a quien se asigna la resolución de la incidencia, documentación sobre la causa y sus efectos.

El régimen de auditoría previsto está recogido en el apartado 5.4.

#### 10.3.8 Copias de respaldo y recuperación

Las copias de respaldo se realizan de forma diaria conforme a la normativa en vigor de la DGP para ordenadores centrales.

Las recuperaciones de datos se hacen con la autorización del responsable del fichero:

- a. Incidencias en el sistema informático: Se comunica al responsable informático del sistema, quien deberá obtener la autorización del propietario mediante los procedimientos establecidos al efecto.
- b. Incidencias en la infraestructura del sistema informático: Se siguen los procedimientos establecidos en los planes de respaldo del Departamento de Sistemas de Información para cada contingencia.

### **10.3.9 Control de accesos**

Las autorizaciones de acceso a los sistemas de información estarán basadas exclusivamente en el principio de necesidad para el trabajo. Los administradores de usuarios y de elementos se encargarán de validar siempre esta necesidad antes de conceder el acceso a los datos.

Asimismo, todos los elementos que permitan acceder a datos personales estarán catalogados como de uso restringido.

El registro de acceso se hace siempre de acuerdo a lo establecido en el artículo 24 del Reglamento de Medidas de Seguridad y recogido en el Documento de Seguridad del Sistema del Documento Nacional de Identidad.

### **10.3.10 Ficheros temporales**

El software utilizado para generar un certificado electrónico conforme al estándar X.509v3 genera ficheros temporales, ficheros de registros de auditoría, que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

El tratamiento de los ficheros temporales está sometido a lo preceptuado en el artículo 7 del Reglamento de Medidas de Seguridad y recogido en el Documento de Seguridad del Sistema del Documento Nacional de Identidad.

### **10.3.11 Gestión de soportes**

Los soportes internos están correctamente identificados por su código de barras o incluyen su correspondiente etiqueta identificativa.

Los soportes están ubicados en las salas de ordenadores. El acceso a estas salas está restringido, las autorizaciones permanentes son validadas por el Jefe del Departamento de Sistemas de Información y el acceso provisional solo podrá ser autorizado por el Jefe de Explotación o el Jefe de Operación.

Todos los soportes que deban salir de los locales de la DGP cumplirán los siguientes requisitos:

- La salida estará autorizada por el Administrador de la PKI, manteniéndose a estos efectos por el Departamento de Sistemas de Información un registro en papel de la entrada/salida de soportes

- Estos soportes estarán protegidos mediante técnicas criptográficas, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.
- Las salidas por mantenimiento de soportes se someterá a un proceso de borrado físico o desmagnetización.,

La reutilización de soportes que hubieran contenido datos de carácter personal se someterán a un proceso de borrado físico o similar.

### **10.3.12 Utilización de datos reales en pruebas**

No se utilizarán datos personales reales para la realización de pruebas, salvo que se aseguren los mismos niveles de seguridad que establece la presente DPC.

Los procedimientos de pruebas utilizados en el Departamento de Sistemas de Información aseguran el cumplimiento del nivel de seguridad requerido para la utilización de datos reales en pruebas.

## ÚLTIMOS CAMBIOS

### LISTA DE ÚLTIMOS CAMBIOS

■ **Apartado:**

Cambio:

- Cambio
- Cambio

■ **Apartado:**

Cambio:

- Cambio
- Cambio

■ **Apartado:**

Cambio:

- Cambio
- Cambio