INFRAESTRUCTURA DE CLAVE PÚBLICA

DNI ELECTRÓNICO Y FIRMA CENTRALIZADA

DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN

OID: 2.16.724.1.2.2.2.1.2.9

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

NOTA INFORMATIVA

De acuerdo con la información publicada por parte de los principales organismos especializados en la seguridad de la información, incluyendo el CERT-EU, y siguiendo las recomendaciones del Centro Criptológico Nacional, en relación con la reciente publicación de la vulnerabilidad ROCA que afecta a determinados productos utilizados por el DNIe 2.0 y 3.0, y con objeto de garantizar la seguridad y confianza de los usuarios del DNIe, se procede, en los soportes preexistentes afectados ,y a partir del ASG160001, a la generación de nuevos certificados con longitudes de claves RSA de 1920 bits con un periodo de vigencia máxima de 24 meses no renovables desde la fecha de su expedición. Para la expedición en nuevos soportes, se procederá a la generación de certificados con longitudes de claves RSA de 2048 bits con un periodo de vigencia máxima de 24 meses renovables por periodos de la misma validez hasta la caducidad del documento.

En los soportes no afectados ya expedidos, se mantendrán las longitudes de claves RSA de 2048 bits con un periodo máximo de vigencia de hasta 60 meses desde la fecha de su expedición.

Por último, en el caso de renovación de certificados en soportes no afectados, se procederá a la generación de certificados con longitudes de claves RSA de 2048 bits con un periodo de vigencia máxima de 24 meses renovables por periodos de la misma validez hasta la caducidad del documento.

1. INTRODUCCIÓN

1.1 RESUMEN

Desde el 1 de julio de 2016 es de aplicación el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, transposición al Ordenamiento jurídico español 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, se encuentra desde entonces jurídicamente desplazada por el citado Reglamento en todo aquello regulado por él, hasta su derogación final a través de la futura Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, del que existe en la actualidad un anteproyecto de Ley.

Asimismo, la actual **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.

En este sentido, el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, comprende medidas relativas a la documentación nacional de identidad dirigidas a configurar el Documento Nacional de Identidad, con carácter exclusivo y excluyente, como el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular, modificando el apartado 1 del artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y el apartado 1 del artículo 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Por otro lado, el documento nacional de identidad electrónico destaca por el cumplimiento con los requisitos de reconocimiento mutuo por parte de organismos del sector público de los Estados miembros a efectos de autenticación trasfronteriza del servicio prestado en línea por dichos organismos de acuerdo con el artículo 6 del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y permite la realización de firmas electrónicas cualificadas según normativa de aplicación.

Este nuevo mecanismo de identificación basado en el actual Documento Nacional de Identidad, cuya expedición se regula, entre otros, por el Real Decreto 1553/2005, de 23 de diciembre, (modificado por el RD 869/2013 y RD 414/2015), y que 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 70 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 – ha implantado una Infraestructura de Clave Pública, que dota al nuevo DNI de los certificados electrónicos necesarios para cumplir adecuadamente con los objetivos anteriores.

La Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, establece que el sistema Cl@ve permitirá el acceso a servicios de firma en la nube (en adelante firma centralizada) basados en certificados electrónicos centralizados.

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 DNI) para ciudadanos españoles, así como de los Certificados de firma electrónica centralizados del Documento Nacional de Identidad para ciudadanos españoles y extranjeros (en adelante se refiere a ciudadanos con NIE junto con alguno de los documentos oficiales que lo acredite, siendo los únicos permitidos el Certificado de Registro de Ciudadano de la Unión o la Tarjeta de Extranjero). 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 estándares europeos, entre los que cabe destacar los siguientes:

- ETSI EN 319 411-2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.

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

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- Ley 84/78, 28 de Diciembre que regula la tasa por expedición y renovación del DNI.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- 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.
- Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el 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.
- Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el 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.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.
- Real Decreto 414/2015, de 29 de mayo, por el que se modifica el 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 Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, Título I, Capítulo I, Artículos 3 y 4.
- Real Decreto 557/2011, de 20 de abril por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, Título XIII, Capítulo I, Artículos 205 y 206, Capítulo II, Artículos 207-210 y Capítulo IV, Artículos 213 y 214.
- Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España en ciudadanos de los Estados miembros de la Unión Europea y de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo.
- Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, concretamente ANEXO I Secretaria de Estado de Seguridad, Dirección General de Policía, Ámbito del Cuerpo Nacional de Policía, Punto 3: Adexttra.
- Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones, por las que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

La regulación vigente en España, en la fecha de elaboración del presente documento de prácticas y políticas de certificación, continúa siendo la Ley de Firma Electrónica 59/2003 en aquellos aspectos que complementen al Reglamento (UE) 910/2014.

Esta ley ha tenido innumerables efectos beneficiosos si bien no ha conseguido los objetivos fijados en cuanto al uso masivo de la firma electrónica cualificada. Dicho nivel de firma tiene la máxima eficacia legal de manera que su utilización otorga una equivalencia automática con la firma manuscrita.

En el ámbito de las AAPP el uso estricto de las firmas electrónicas cualificadas es inferior a lo esperado, debido a que las tecnologías necesarias para cualificar la firma electrónica exigen en la práctica la utilización de un dispositivo de creación de firma electrónico certificado como dispositivo cualificado de creación de firma electrónica.

En el anexo de la Decisión de ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 figuran las normas para la evaluación de la seguridad de productos de tecnología de la información que se aplican a la certificación de dispositivos cualificados de creación de firma electrónica o dispositivos cualificados de creación de sello electrónico de conformidad con el artículo 30, apartado 3, letra a), o con el artículo 39, apartado 2, del Reglamento (UE) nº 910/2014, cuando los datos de creación de firma electrónica o los datos de creación de sello electrónico se conservan íntegramente, aunque no necesariamente de forma exclusiva, en un entorno gestionado por el usuario.

Entre la lista de normas referidas en el anexo se cita la familia EN 419 211 — Protection profiles for secure signature creation device (Perfiles de protección para los dispositivos seguros de creación de firma), Partes 1 a 6, siendo la versión actual del dispositivo cualificado de creación de firma electrónica del DNI electrónico (versión 3.0) conforme con los perfiles de protección «Protection profiles for Secure signature creation device - Part 2: Device with key generation», versión 2.0.1 (EN 419211-2:2013) y «Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application», versión 1.0.1 (EN 419211-5:2013).

En este contexto, los Certificados de Identidad Pública y firma electrónica del Documento Nacional de Identidad (DNI) almacenados en el chip del DNI electrónico, para ciudadanos españoles, y los Certificados de firma centralizada del Documento Nacional de Identidad, para ciudadanos españoles y extranjeros, serán emitidos como **Certificados Electrónicos Cualificados** cumpliendo los requisitos de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica que complementen los requisitos establecidos en el artículo 28 y anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. El prestador de servicios de confianza, Dirección General de la Policía (Ministerio del Interior), cumplirá los requisitos expresados en el artículo 24 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y aquellos aspectos que complemente la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

En este sentido, en el artículo 51 del Reglamento (UE) 910/2014 establece en el apartado segundo que, los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán **certificados cualificados** de firma electrónica con arreglo al presente Reglamento hasta que caduquen.

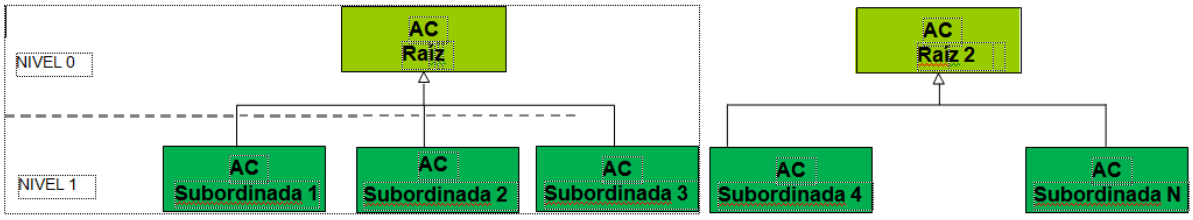
Asimismo, se han tenido en cuenta los estándares en materia de certificados cualificados, en concreto:

- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

De acuerdo con la legislación señalada, se considera firma electrónica cualificada la firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica. La firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.

La arquitectura general, a nivel jerárquico de la PKI del DNI y firma centralizada es la siguiente:



- Un primer nivel en el que se ubica las AC raíz que representan el punto de confianza de todo el sistema y que permitirá, tal y como recoge el artículo 15 de la Ley de Firma electrónica y en la ley 39/2015, que todas la personas físicas o jurídicas, públicas o privadas, reconozcan la eficacia del Documento Nacional de Identidad electrónico para acreditar la identidad. Por otro lado, la Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, establece que el sistema Cl@ve permitirá el acceso a servicios de firma centralizada basados en certificados electrónicos centralizados.
- Un segundo nivel, constituido por las AC subordinadas de las ACs Raíz que emitirán los certificados de identidad pública y firma electrónica del Documento Nacional de Identidad (DNI) para ciudadanos españoles así como los certificados de firma centralizada del Documento Nacional de Identidad para ciudadanos españoles y extranjeros.

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 del DNI electrónico para ciudadanos españoles así como los certificados de firma centralizada para ciudadanos españoles y extranjeros.

Esta DPC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos almacenados, en su caso, en el chip del DNI o en el dispositivo centralizado, en todo su ciclo de vida, y sirve de guía de la relación entre los certificados del DNI, los de firma centralizados 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.

Esta DPC también 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.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre del documento	Declaración de Prácticas y Políticas de Certificación (DPC)
Versión del documento	2.9
Estado del documento	Aprobado
Fecha de emisión	27/07/2020
Fecha de caducidad	No aplicable
OID (Object Identifier)	2.16.724.1.2.2.2.1.2.9
Ubicación de la DPC	http://www.dnie.es/dpc http://pki.policia.es/dnie/publicaciones/dpc

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 DNI para ciudadanos españoles y de los certificados de firma centralizada para ciudadanos españoles y extranjeros.
- La Autoridad de Aprobación de Políticas.
- Las Autoridades de Certificación.
- Las Autoridades de Registro.
- Las Autoridades de Validación.
- Prestadores de Servicios de Confianza.
- Los ciudadanos como solicitantes del DNI para ciudadanos españoles y de los certificados de firma centralizada para ciudadanos españoles y extranjeros.
- Los ciudadanos titulares del DNI para ciudadanos españoles y de los certificados de firma centralizada para ciudadanos españoles y extranjeros.
- Los Terceros Aceptantes de los certificados emitidos por DNI para ciudadanos españoles y de los certificados de firma centralizada para ciudadanos españoles y extranjeros incluyendo Prestadores de Servicios basados en la utilización del DNI para ciudadanos españoles y de los certificados de firma centralizada para ciudadanos españoles y extranjeros.

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, o en su defecto por la propia Autoridad de Aprobación de Políticas.

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 DNI y de los certificados de firma centralizada, de determinar la adecuación de la DPC de dicha AC a esta DPC y de regular 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 DNI y de los certificados de firma centralizada, así como de solicitar, en caso necesario, la implementación de acciones correctoras.

1.3.2 Autoridades de Certificación

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

Las Autoridades de Certificación que componen la PKI son:

Actual jerarquía:

- "**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:

Nombre Distintivo	CN= AC RAIZ DNIE, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Certificado pkcs1-sha256WithRSAEncryption	
Número de serie	00 c5 26 c9 6e 10 94 ed 43 4f f7 b5 fb 67 9f 94
Periodo de validez	Desde jueves, 16 de febrero de 2006 11:37:25 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

- **"AC Raíz 2"**: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma, su Autoridad de Validación y la Autoridad de Revocación y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones que se establece.

  Sus datos más relevantes son:

Nombre Distintivo	CN= AC RAIZ DNIE 2, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
sha256WithRSAEncryption	
Número de serie	2b 1b bb cb 61 cf 48 24 52 45 5d 3d 5e db e2 a3
Periodo de validez	Desde viernes, 27 de septiembre de 2013 11:26:05 hasta domingo, 27 de septiembre de 2043 11:26:05
Huella Digital (SHA-1)	eb 4d 69 02 fd 60 ec d5 0e e5 8e 2c 9f 20 29 2c 39 10 27 ce

- **"AC Subordinadas"**: Autoridades de Certificación subordinadas de las "AC Raíz". Su función es la emisión de certificados para los titulares de DNI y de los certificados de firma centralizada.

  En el momento de publicación de la presente DPC, el dominio de certificación del DNI 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
Emisor	CN= AC RAIZ DNIE, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
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

Autoridad de Certificación Subordinada 002

Nombre Distintivo	CN= AC DNIE 002, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Emisor	CN= AC RAIZ DNIE, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Certificado pkcs1- sha256WithRSAEncryption	
Número de serie	3e 02 bf 5b de 8e 3d 16 44 05 7e fa 56 4c 42 75
Periodo de validez	Desde miércoles, 01 de marzo de 2006 12:01:14 Hasta viernes, 26 de febrero de 2021 23:59:59
Estado	Operativa
Huella Digital (SHA-1)	50 2b d0 07 8e 6d a2 35 c4 5f 52 1c 63 ef 54 9d f0 19 8f dd

Huella Digital (MD5)	5b 6a a3 c5 7a 68 9a eb 7d 29 70 1e 91 9c 4f 96

Autoridad de Certificación Subordinada 003

Nombre Distintivo	CN= AC DNIE 003, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Emisor	CN= AC RAIZ DNIE, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Certificado pkcs1- sha256WithRSAEncryption	
Número de serie	08 f7 7b 06 6f b6 1b cd 44 05 7f 51 2e 0a db a8
Periodo de validez	Desde miércoles, 01 de marzo de 2006 12:02:41 Hasta viernes, 26 de febrero de 2021 23:59:59
Estado	Operativa
Huella Digital (SHA-1)	fb c0 71 d0 a4 81 11 bd df 77 76 d0 9e 42 bc 53 4e 24 48 70
Huella Digital (MD5)	67 a1 0e 56 91 c8 c5 8b e5 ba 91 8c ce 90 e8 7e

Autoridad de Certificación Subordinada 004

Nombre Distintivo	CN= AC DNIE 004, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Emisor	CN= AC RAIZ DNIE 2, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
sha256WithRSAEncryption	
Número de serie	43 9a 96 28 b2 66 0f ee 53 9a eb 66 fc f1 55 18
Periodo de validez	Desde viernes, 13 de junio de 2014 13:15:34 Hasta miércoles, 13 de junio de 2029 13:15:34
Estado	Operativa
Huella Digital (SHA-1)	3f 7a 70 b9 82 73 db 7e 02 6b 95 da 49 e9 b6 93 0d 65 82 9a

Autoridad de Certificación Subordinada 005

Nombre Distintivo	CN= AC DNIE 005, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Emisor	CN= AC RAIZ DNIE 2, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
	sha256WithRSAEncryption
Número de serie	68 fc 4e 19 57 a3 d0 05 55 81 44 c1 43 58 0b dd
Periodo de validez	Desde miércoles, 17 de junio de 2015 10:58:25 Hasta lunes, 17 de junio de 2030 10:58:25
Estado	Operativa
Huella Digital (SHA-1)	e7 0c f3 b6 c8 56 76 29 b6 9b e8 c9 5d 63 d9 04 00 85 c1 95

Autoridad de Certificación Subordinada 006

Nombre Distintivo	CN= AC DNIE 006, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Emisor	CN= AC RAIZ DNIE 2, OU=DNIE, O=DIRECCION GENERAL DE LA POLICIA, C=ES
	sha256WithRSAEncryption
Número de serie	26 7d ea b7 26 5c 1b c0 55 b7 79 e1 41 09 f0 42
Periodo de validez	Desde martes, 28 de julio de 2015 13:47:29 Hasta domingo, 28 de julio de 2030 13:47:29
Estado	Operativa
Huella Digital (SHA-1)	42 3b b4 97 39 ea 4e 1b e6 f4 71 61 ea b8 97 7b f6 55 b7 ee

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

En el ámbito del DNI, 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 procedimiento 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 DNI.

Por otro lado, en el ámbito de los certificados de firma centralizada, la Autoridad de Registro está constituida por todas las oficinas de la Agencia Estatal de Administración Tributaria, (AEAT) y de las Entidades Gestoras y Servicios Comunes de la Seguridad Social 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 registro. En cualquier caso, la DGP a través de las oficinas constituidas a tal efecto, podrá realizar labores de Autoridad de Registro siempre que estime oportuno. Serán oficinas de registro aquellas oficinas de la Administración Pública Estatal habilitadas para actuar como tal en el sistema Cl@ve.

1.3.4 Autoridad de Validación

La(s) Autoridad(es) de Validación (AV) tienen como función la comprobación del estado de los certificados emitidos para el DNI para ciudadanos españoles y extranjeros, 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."* y artículo 24 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

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

- **Ministerio de Hacienda y Función Pública**, utilizará para las repuestas de validación (OCSP) del DNI, el certificado utilizado para la verificación de los Servicios de Firma electrónica e Identidad digital de la plataforma @firma.
- **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 Confianza.

La información del estado de revocación se hará disponible más allá del periodo de validez del certificado durante el periodo de tiempo establecido por la normativa en vigor.

En el caso de compromiso de la clave privada de una Autoridad de Certificación o el cese de actividad del TSP, se proporcionará información del estado de revocación a través de los métodos/servicios de consulta habilitados al efecto conforme la DPC/PC.

1.3.5 Prestador de Servicios de Confianza

En el ámbito de los certificados de firma centralizada.

La Dirección General de la Policía, en adelante DGP, actúa como prestador cualificado de servicios de confianza, emitiendo los certificados electrónicos cualificados de firma y proveyendo servicios de firma electrónica basada en un certificado cualificado y creada mediante un dispositivo cualificado de creación de firma electrónica, conforme a lo establecido en el reglamento 910/2014 de la Unión Europea y en la Ley 59/2003 de Firma electrónica.

La GISS, con el fin de garantizar la continuidad de los servicios, actuará como prestador cualificado de servicios de confianza, junto con la DGP responsable último de la prestación segura del servicio, proveyendo servicios de firma electrónica basada en un certificado cualificado y creada mediante un dispositivo cualificado de creación de firma electrónica, conforme a lo establecido en el reglamento 910/2014 de la Unión Europea y en la Ley 59/2003 de Firma electrónica.

1.3.6 Ciudadano

En el ámbito del DNI y 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.

Por otro lado, en el ámbito del certificado de firma centralizada y a los efectos de esta DPC, se entiende como ciudadano a toda persona física que cumpla con los requisitos legales y que en nombre propio, tras previa identificación, solicita la expedición o renovación del certificado de firma centralizada.

1.3.7 Ciudadano titular del DNI o certificado de firma centralizada

En el ámbito del DNI, 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.

En el ámbito del certificado de firma centralizada, se entiende por usuario del certificado de firma centralizada al ciudadano español y extranjero, mayor de edad y con plena capacidad de obrar, que voluntariamente confía y hace uso del certificado emitido por la Dirección General de la Policía (Ministerio del Interior), del cual es titular. Por ciudadanos extranjeros se refiere a ciudadanos con NIE junto con alguno de los documentos oficiales que lo acredite, siendo los únicos permitidos el Certificado de Registro de Ciudadano de la Unión o la Tarjeta de Extranjero.

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

1.3.8 Terceros aceptantes

Los Terceros Aceptantes son las personas o entidades diferentes del titular que deciden aceptar y confiar en un certificado del DNI o de firma centralizado emitido por la Dirección General de la Policía (Ministerio del Interior).

Por otro lado, tal y como recoge la Ley de Firma electrónica en su articulado, "***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."*

Al mismo tiempo la ley 39/2015 establece que las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

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

1.4 USO DE LOS CERTIFICADOS

1.4.1 Usos apropiados de los certificados

Los Certificados de Identidad Pública y firma electrónica del Documento Nacional de Identidad (DNI), 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 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).

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

  Asimismo, el documento nacional de identidad electrónico destaca por el cumplimiento con los requisitos de reconocimiento mutuo por parte de organismos del sector público de los Estados miembros a efectos de autenticación trasfronteriza del servicio prestado en línea por dichos organismos de acuerdo con el artículo 6 del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014. (DOUE 2018/C 401/08)

  Por otro lado, este certificado tiene en cuenta los requisitos de la política NCP+ según establece la norma europea EN 319 411-1.

- **Certificado de Firma:** El propósito de este certificado es permitir al ciudadano firmar trámites o documentos. Este certificado (certificado cualificado según el Reglamento (UE) 910/2014) permite sustituir la firma manuscrita por la electrónica en las relaciones del ciudadano con terceros (Artículo 25 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior).

  El Reglamento (UE) 910/2014 establece que los certificados cualificados de firma electrónica cumplirán los requisitos establecidos en el anexo I. Por otro lado, la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

  Los certificados de firma son certificados cualificados de acuerdo con lo que se establece en el artículo 28 y anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior así como en aquellos artículos de la Ley 59/2003, de 19 de diciembre, de firma electrónica) que complementen.

  Por otro lado, este certificado tiene en cuenta los requisitos de la política QCP-n-qscd según establece la norma europea EN 319 411-2.Son certificados cualificados que se utilizan en dispositivo cualificado de creación de firma electrónica, de acuerdo con el artículo 29 y anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. 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 cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha estado generada utilizando un dispositivo cualificado de creación de firma electrónica, por lo cual, de acuerdo con lo que establece el artículo 25 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, tendrá un efecto jurídico equivalente al de una firma manuscrita, 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).

Dado que, técnicamente es posible la disociación de los certificados contenidos en el documento nacional de identidad electrónico, el Real Decreto 869/2013, de 8 de noviembre, introduce una modificación al decreto regulador del documento nacional de identidad (1553/2005), a fin de permitir que todos los ciudadanos españoles puedan acreditar su identidad por medios electrónicos, al tiempo que se reserva la capacidad de realizar la firma electrónica de documentos a las personas con capacidad legal para ello.

Este RD establece que "en el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado".

También se establece que "la activación del certificado de firma electrónica en el documento nacional de identidad tendrá carácter voluntario y su utilización se realizará mediante una clave personal y secreta que el titular del documento nacional de identidad podrá introducir reservadamente en el sistema".

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 DNI. De esta forma garantiza que el documento proviene de un determinado ciudadano.

  Dado que el DNI es un dispositivo cualificado de creación de firma electrónica 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.

Por otro lado, el Certificado de firma centralizada del Documento Nacional de Identidad emitido a ciudadanos españoles y extranjeros por la Dirección General de la Policía (Ministerio del Interior) tendrá como finalidad:

- **Certificado de firma centralizado:** El propósito de este certificado es permitir al ciudadano firmar trámites o documentos. Este certificado es un certificado cualificado según el Reglamento (UE) 910/2014.

  El Reglamento (UE) 910/2014 establece que los certificados cualificados de firma electrónica cumplirán los requisitos establecidos en el anexo I. Por otro lado, la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

  Los certificados de firma son certificados cualificados de acuerdo con lo que se establece en el artículo 28 y anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior así como en aquellos artículos de la Ley 59/2003, de 19 de diciembre, de firma electrónica) que complementen.

  Por otro lado, este certificado tiene en cuenta los requisitos de la política QCP-n según establece la norma europea EN 319 411-2.

El uso del certificado de firma proporciona las siguientes garantías:

- 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 certificado de firma centralizado. De esta forma garantiza que el documento proviene de un determinado ciudadano.

  Dado que en el sistema de firma con certificados centralizados se garantiza que las claves de firma permanecen, con un alto nivel de confianza, 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 Centralizado, 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), en caso de DNI y para firmar electrónicamente (no repudio y compromiso con lo firmado) en caso de los certificados de firma centralizados.

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).

Los usos de las claves de las Autoridades de Certificación se limitan a la firma de certificados, generación de CRLs y OCSP.

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).

Los servicios de confianza que ofrece DNI y de certificados de firma centralizados, 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 DNI es un dispositivo cualificado de creación de firma electrónica y como tal, garantiza que las claves permanecen desde el momento de su creación bajo el control del ciudadano titular del DNI 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.

Por otro lado, se garantiza que las claves de firma permanecen, con un alto nivel de confianza, bajo el control del ciudadano titular del certificado de firma centralizada. El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de las claves de acceso al certificado, evitando su pérdida, divulgación, modificación o uso no autorizado.

1.4.3 Fiabilidad de la firma electrónica a lo 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 por 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 DNI y de los certificados de firma centralizados

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

Nombre	Dirección General de la Policía (Ministerio del Interior)		
Dirección e-mail	certificados@dnielectronico.es		
Dirección	C/Miguel Ángel 5 MADRID (España)		
Teléfono	+34913223400	**Fax**	+34913085774

1.5.2 Persona de contacto

Esta DPC está administrada por la Autoridad de Aprobación de Políticas (AAP) del DNI Electrónico y de los certificados de firma centralizados.

Nombre	Grupo de trabajo del Certificado de Identidad Pública		
Dirección e-mail	certificados@dnielectrónico.es		
Dirección	C/Miguel Ángel 5 MADRID (España)		
Teléfono	+34913223400	**Fax**	+34913085774

1.5.3 Determinación de la adecuación de la DPC de una AC externa a las Políticas de Certificación de DNI y de los certificados de firma centralizados

En el caso de que se tuviese que evaluar la posibilidad de que una AC externa interactúe con la PKI del DNI y de los certificados de firma centralizados estableciendo relaciones de confianza, la Autoridad de Aprobación de Políticas (AAP) de DNI y de los certificados de firma centralizados 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 DNI y de los certificados de firma centralizados 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 DNI el dato de activación es la clave personal de acceso (PIN) y/o los patrones de las impresiones dactilares (biometría).

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de confianza que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Certificados de Identidad Pública: Emitidos como Certificados Cualificados, 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.

Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014.

Certificados de firma electrónica centralizados: emitidos como Certificados cualificados, vinculan una serie de datos personales del ciudadano a unas determinadas claves, para garantizar la integridad y no repudio. Esta información está firmada electrónicamente por la Autoridad de Certificación creada al efecto.

Ciudadano: Ver apartado 1.3.6 de la DPC.

Clave Pública y Clave Privada: la criptografía asimétrica en la que se basa la PKI emplea un par de claves de modo 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 de un solo uso (OTP): código de un solo uso (One Time Password) enviado para el registro y uso en el sistema Cl@ve.

Código de activación: Código suministrado en el proceso de Registro en el sistema Cl@ve.

Cl@ve permanente: Sistema de autenticación diseñado para personas que necesitan acceder frecuentemente a los servicios electrónicos de la Administración. Se basa en el uso de un código de usuario, su DNI o NIE, y de una contraseña que se establece en el proceso de activación y que sólo debe ser conocida por el ciudadano. Para los servicios de administración electrónica que requieran un nivel de seguridad elevado, el sistema refuerza la autenticación con la solicitud de introducción de un código numérico de un solo uso (OTP).

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

Datos de creación de Firma (Clave Privada): son datos únicos, como códigos o claves criptográficas privadas, que el firmante 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 cualificado de creación de Firma: un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014.

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, por la DGP como Prestador de Servicios de Confianza, 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 u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

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 firmante respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al firmante, como a los datos a que se refiere, y por haber sido creada por medios que mantiene, con un alto nivel de confianza, bajo su exclusivo control.

Firma electrónica cualificada: es aquella firma electrónica avanzada basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma electrónica.

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 DNI y certificados de firma centralizados.

Identificación electrónica: el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física.

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 DNI y certificados de firma centralizados, 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.

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

Prestador de servicios de confianza: una persona física o jurídica que presta uno o más servicios de confianza.

Prestador cualificado de servicios de confianza: prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.

Punto de Actualización del DNI: 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 DNI (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 para el DNI o certificados de firma centralizados.

Titular: ciudadano para el que se expide un certificado de identidad pública y de firma electrónica. Para más detalles, ver apartado 1.3.7 de la DPC.

1.6.2 Acrónimos

AAP: Autoridad de Aprobación de Políticas.

AEAT: Agencia Estatal de la Administración Tributaria.

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

DGP: Dirección General de la Policía.

DPC: Declaración de Prácticas y Políticas de Certificación.

ETSI: European Telecommunications Standard Institute.

FIPS: Federal Information Processing Standard (Estándar USA de procesado de información).

GISS: Gerencia de Informática de la Seguridad Social.

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).

NIE: Número de Identidad de Extranjero.

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

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

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

PKIX: Grupo de trabajo dentro del IETF (Internet Engineering Task Group) constituido con el objeto de desarrollar las especificación relacionadas con las PKI e Internet.

PSC: Prestador de Servicios de Confianza.

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.

TSP: Trust Service Providers.

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

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[1]
- WEB: http://pki.policia.es/dnie/certs/ACRaiz2.crt
- WEB: http://pki.policia.es/dnie/certs/ACXXX.crt[2]

Para la lista de AC revocadas (ARL):

- WEB: http://crls.dnie.es/crls/ARL.crl
- WEB: http://pki.policia.es/dnie/crls/ARL.crl

Para la DPC:

- WEB: http://www.dnie.es/dpc
- WEB: http://pki.policia.es/dnie/publicaciones/dpc

Desde la página se accede a los siguientes documentos:

- Términos y condiciones (http://www.dnie.es/terminos y http://pki.policia.es/dnie/publicaciones/terminos)

Servicio de validación en línea que implementa el protocolo OCSP:

- WEB: http://ocsp.dnie.es

Los certificados de validación de las respuestas OCSP se encuentran publicados en el sitio web https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_079.

El repositorio de DNI y de los certificados de firma centralizados 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 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/ 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 DNI y de los certificados de firma centralizados 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.

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 DNI y de los certificados de firma centralizados se llevará a cabo con anterioridad al comienzo de la prestación del servicio

[1] XXX identificador numérico de tres dígitos de la AC subordinada.

[2] XXX identificador numérico de tres dígitos de la AC subordinada.

en la dirección de Internet del DNI y de los certificados de firma centralizados (http://www.dnielectronico.es/) o 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 presente DPC, éstas se notificarán en la dirección de Internet (http://www.dnielectronico.es/).

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, términos y condiciones) es abierto, pero sólo la AAP del DNI y de los certificados de firma centralizados está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello DNI y los certificados de firma centralizados establecerán 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 de DNI y para firma centralizada 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 ámbito del DNI, 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

En el ámbito del certificado de firma centralizada, el DN del 'subject name' incluye los siguientes campos:

CN=<APELLIDO1> <APELLIDO2>, <NOMBRE> (FIRMA CENTRALIZADA)

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) | <NIE> (con letra)

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 para el DNI y los certificados de firma centralizada para interpretar los nombres distintivos de los titulares de certificados que emite es ISO/IEC 9595 (X.500) Distinguished Name (DN).

La RFC 5280 ("*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 para el DNI y para la de firma centralizada, 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 DNI del ciudadano garantiza la unicidad del DN.

Los DN del certificado de autenticación y de firma del DNI 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.

Por otro lado, para garantizar la unicidad del DN en el ámbito de los certificados de firma centralizada se incluirá el literal (FIRMA CENTRALIZADA) en el Common Name (CN) 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

En el ámbito del DNI, 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 cualificado de creación de firma electrónica (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 DNI. 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 DNI.

Por otro lado, en el ámbito del certificado de firma centralizada, una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro, ha activado su Cl@ve Permanente, y ha solicitado expresamente la emisión de sus certificados de firma centralizada, dicha emisión se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma.

El sistema informará al ciudadano de que se le va a emitir su certificado de firma centralizada y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial.

3.2.2 Autenticación de la identidad de una persona jurídica

No estipulado.

3.2.3 Autenticación de la identidad de una persona física

En el ámbito del DNI, 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 DNI con la documentación que se establece en el Real Decreto ***1553/2005***, y en sus modificaciones por Reales Decretos 1586/2009 y 869/2013, así como en el apartado 4.2 de esta DPC, acompañado de la persona que tenga encomendada la patria potestad o tutela (o persona apoderada por estas últimas) cuando éste sea menor de 14 años o sea una persona con capacidad judicialmente complementada.

En el caso especial de incapacitados que no puedan acudir a una Oficina de Expedición, podrán obtener su DNI 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 DNI. 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 cualificados 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.

En cualquier momento, sin que medie la extinción de la vigencia del soporte (tarjeta), podrá solicitarse la expedición de nuevos certificados cualificados, 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 DNI 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.

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.

Por otro lado, en el ámbito del certificado de firma centralizada, la identificación y autenticación del ciudadano para la solicitud del Certificado seguirá un proceso integrado con el registro previo en el censo de usuarios de Cl@ve.

Para el registro se aportará la información complementaria que se establezca en el procedimiento de registro del sistema Cl@ve.

3.2.4 Información no verificada sobre el solicitante

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

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, el certificado de identidad y, si procede, el de firma electrónica del DNI, deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o sea una persona con capacidad judicialmente complementada, se llevará a cabo en presencia de quien tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas.

En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.

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 Confianza (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

En el ámbito del DNI, 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 DNI) 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.

En el ámbito del certificado de firma centralizada, la renovación del certificado se podrá llevar a cabo de forma que se cumplan los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial. En caso contrario, para renovar su certificado el ciudadano tendrá que personarse en una oficina de registro siguiendo los procedimientos de comprobación de la identidad del ciudadano desarrollados a tal efecto.

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) así como firma centralizada.

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Quién puede efectuar una solicitud

En el ámbito del DNI, 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 DNI, como recoge el Real Decreto ***1553/2005***, en su modificación introducida por el Real Decreto 869/2013, 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. En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá únicamente la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.

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.

Por otro lado, en el ámbito del certificado de firma centralizada, toda persona física, mayor de edad, y que en nombre propio cumpla con los requisitos legales, tras previo registro en el censo de usuarios de Cl@ve, puede solicitar la expedición del certificado.

4.1.2 Registro de las solicitudes de certificados

En el ámbito del DNI, 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 DNI y por tanto los Certificados asociados deberá acudir a una Oficina de Expedición del DNI. La relación de equipos fijos de expedición está accesible en el sitio web: www.dnielectronico.es. A determinadas 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 DNI (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 seis meses a la fecha de presentación de la solicitud de expedición del Documento Nacional de Identidad y que contengan la anotación de que se ha emitido a los solos efectos de la obtención de este documento.

b) Una fotografía reciente en color del rostro del solicitante, tamaño 32 por 26 milímetros, con fondo uniforme blanco y 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 o volante 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 al certificado de identidad y, en su caso, al de 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 personal 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.

Por otro lado, en el ámbito del certificado de firma centralizada, el registro de las solicitudes de certificado se realizará a través de las Autoridades de Registro constituidas por todas las oficinas de la Agencia Estatal de Administración Tributaria (AEAT) y de las Entidades Gestoras y Servicios Comunes de la Seguridad Social. En cualquier caso, la DGP a través de las oficinas constituidas a tal efecto, podrá realizar labores de Autoridad de

Registro siempre que estime oportuno. Serán oficinas de registro aquellas oficinas de la Administración Pública Estatal habilitadas para actuar como tal en el sistema Cl@ve.

4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 Realización de las funciones de identificación y autenticación

En el ámbito del DNI, 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 DNI.

Estos funcionarios desempeñan el rol de operador de registro, disponiendo de un dispositivo cualificado de creación de firma electrónica (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.

Por otro lado, en el ámbito del certificado de firma centralizada, las funciones de identificación y autenticación descritas anteriormente las realizan los funcionarios y personal encargado en las Autoridades de Registro constituidas a tal efecto.

4.2.2 Aprobación o denegación de las solicitudes de certificados

En el ámbito del DNI, solo se privará del derecho a la expedición de un DNI y/o a los dispositivos cualificados de creación de firma electrónica que incorpora, en los casos y forma establecidos por el Real Decreto que regula su expedición y otras Leyes de aplicación, en cuyo caso habrá de ser sustituido por otro documento identificador.

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 DNI (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 DNI válida (todas las tarjetas soporte de DNI 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.

Por otro lado, en el ámbito del certificado de firma centralizada, la aprobación/denegación de una solicitud se determina en función del cumplimiento de los requisitos indicados en la propia DPC.

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

En el ámbito del DNI, 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 DNI, 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 de la PKI del DNI 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.

Por otro lado, en el ámbito del certificado de firma centralizada, una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro, ha activado su Cl@ve Permanente, y ha solicitado expresamente la emisión de sus certificados de firma centralizada, dicha emisión se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma.

El sistema informará al ciudadano de que se le va a emitir su certificado de firma centralizada y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial.

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

En el ámbito del DNI, el solicitante conocerá la emisión efectiva de los certificados de identidad pública y firma electrónica con la firma del talón-foto, por parte del solicitante, que acredita la entrega del DNI.

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 mediante el conocimiento previo de los términos y condiciones de la prestación del servicio de confianza, se indicará al ciudadano cómo obtener la presente DPC así como el resto de información requerida por el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE así como de la Ley 59/2003, de 19 de diciembre.

Por otro lado, en el ámbito del certificado de firma centralizada, en la finalización del proceso de generación del certificado de firma se informa al ciudadano que se encuentra disponible dicho certificado para su uso, pudiendo ser usado a partir de ese mismo momento, para los procesos de firma electrónica.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 Forma en la que se acepta el certificado

En el ámbito del DNI, tal y como recoge el Real Decreto ***1553/2005*** en su redacción dada por el Real Decreto 869/2013, la activación de la funcionalidad de firma electrónica del DNI tendrá carácter voluntario, por lo que el ciudadano podrá solicitar la revocación de este certificado como parte del proceso de expedición.

Si el usuario no manifiesta la intención de revocar el certificado de firma electrónica, se dará por confirmada la aceptación del mismo, 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.

Por otro lado, en el ámbito del certificado de firma centralizada, en el caso de generación del certificado de firma electrónica el propio acto de emisión conlleva la aceptación implícita del certificado de firma.

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 los términos y condiciones establecidos 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.

En el ámbito del DNI, 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 cualificada de documentos.

Por otro lado, en el ámbito del certificado de firma centralizada, el Certificado de firma, emitido por la Dirección General de la Policía (Ministerio del Interior) tendrá como finalidad permitir la firma electrónica cualificada 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

En el ámbito DNI, 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:

- Dos años cuando el solicitante no haya cumplido los cinco años de edad.
- Cinco años, cuando el titular haya cumplido los cinco años de edad y no haya alcanzado 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 o, cuando habiendo alcanzado los 30 de edad, acredite tener reconocida la condición de gran inválido.

- Por un año, en ciertos casos excepcionales contemplados en el Real Decreto que regula la expedición del DNI (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 cualificados incorporados al DNI tendrán un período de vigencia no superior a 60 meses [Ver nota informativa], 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 DNI habilitados en las Oficinas de expedición del DNI, siempre que el soporte físico (la tarjeta DNI) no esté dentro del periodo habilitado para solicitar su renovación.
- Renovación a voluntad del titular del DNI sin que medie un cambio de soporte.

  Esta solicitud podrá realizarse desde los Puntos de Actualización del DNI habilitados en las Oficinas de expedición del DNI, siempre que el soporte físico (la tarjeta DNI) no esté dentro del periodo habilitado para solicitar su renovación.

Por otro lado, en el ámbito del certificado de firma centralizada, todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves. Además, los certificados electrónicos cualificados tendrán un período máximo de vigencia de 60 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 permite la renovación con cambio de claves de un certificado por la caducidad de los certificados u olvido de la contraseña establecida en la emisión del certificado.

4.7.2 Quién puede pedir la renovación de un certificado

En el ámbito del DNI, el proceso de renovación de los Certificados sin que medie una renovación del soporte físico deberá ser solicitada de forma voluntaria y por iniciativa del ciudadano.

En los casos de caducidad del soporte del DNI, 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 del certificado de firma como parte del proceso de renovación del soporte.

La DGP como Órgano que tiene atribuidas las competencias del DNI se reserva el derecho de denegar la solicitud de renovación del certificado de firma electrónica cuando el número

de revocaciones sin causa justificada de certificados asociados a un mismo soporte físico (tarjeta DNI) sea superior a 3 en el caso de soportes de 5 años y superior a 5 en el resto de casos.

Por otro lado, en el ámbito del certificado de firma centralizada, la renovación del certificado de firma se podrá llevar a cabo de forma telemática siempre y cuando se cumplan los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial. En caso contrario, para renovar su certificado el ciudadano tendrá que personarse en una oficina de registro para que se le provea de un nuevo código de activación y pueda volver a activarse su usuario y el certificado.

La renovación telemática se producirá cuando el ciudadano que se disponga a firmar, se haya autenticado para poder acceder a su clave de firma y se detecte en ese momento que su certificado está caducado o próximo a caducar, hasta 2 meses antes de la fecha de expiración de su validez. En ese caso el sistema Cl@ve emitirá y almacenará automáticamente los nuevos certificados revocando previamente los antiguos, de acuerdo a la normativa vigente sobre certificados electrónicos cualificados.

En todo caso el sistema informará al ciudadano de que se ha procedido a la renovación telemática de sus certificados y le informará del nuevo periodo de validez de los mismos, informando también de que los anteriores certificados han sido revocados, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

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.

- 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.

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

  En cualquier momento podrá solicitarse la expedición de nuevos certificados cualificados, 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 haciendo uso de los Puntos de Actualización del DNI. Los certificados tendrán como fecha de entrada en vigor el instante en que haya sido generado y como periodo máximo de validez hasta 60 meses (sin superar el periodo de validez del soporte físico) [Ver nota informativa]. Los certificados vigentes hasta el momento serán eliminados de la tarjeta.

  En el ámbito del certificado de firma centralizada, la renovación telemática se producirá cuando el ciudadano que se disponga a firmar, se haya autenticado para poder acceder a su clave de firma y se detecte en ese momento que su certificado está caducado o próximo a caducar, hasta 2 meses antes de la fecha de expiración de su validez. En ese caso el sistema Cl@ve emitirá y almacenará automáticamente los nuevos certificados revocando previamente los antiguos, de acuerdo a la normativa vigente sobre certificados electrónicos cualificados.

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 generado, 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 certificados al titular

En el ámbito del DNI, la notificación se hace con la entrega del nuevo Documento Nacional de Identidad electrónico o mediante la comunicación de la finalización satisfactoria del proceso de renovación cuando no se cambie de soporte.

Por otro lado, en el ámbito del certificado de firma centralizada, en la finalización del proceso de generación del certificado de firma se informa al ciudadano que se encuentra disponible dicho certificado para su uso. En ese momento, se devuelve el control a la aplicación iniciando así el proceso de firma electrónica.

4.7.5 Forma de aceptación del certificado con nuevas claves

En el ámbito de DNI, en el caso de renovación de los certificados tras un cambio en el soporte, si el usuario no manifiesta la intención de revocar el certificado de firma, se dará por confirmada la aceptación del mismo, así como de sus términos y condiciones.

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

Por otro lado, en el ámbito del certificado de firma centralizada, en los casos de renovación de los certificados 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

En el ámbito del DNI, 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 que se tratarán como una renovación del soporte por variación de datos, siendo de aplicación los apartados anteriores.

En el ámbito del certificado de firma centralizada, la modificación de un certificado, implica la invalidación del certificado actual y la emisión de un nuevo certificado.

4.9 REVOCACIÓN DE CERTIFICADOS

La revocación del certificado de firma electrónica, así como los certificados de firma centralizada 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.

En el ámbito del DNI, como regla general la pérdida de validez del soporte del Documento Nacional de Identidad (tarjeta) llevará aparejada la pérdida de validez de los certificados cualificados 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 (autenticación, firma y firma centralizada) y la expedición del certificado de autenticación y, en su caso, del certificado de firma.

4.9.1 Causas para la revocación

Los certificados de identidad pública y firma electrónica, así como los certificados de firma centralizada pueden ser revocados por:

- Renuncia del ciudadano al sistema, excepto respecto del certificado de identidad.
- Sustracción, extravío, destrucción o deterioro del DNI soporte del Certificado.
- Tras la renovación por variación de los datos.
- Incapacidad sobrevenida o fallecimiento del titular del DNI o del certificado de firma centralizada.
- Inexactitudes graves en los datos aportados por el ciudadano para la obtención del DNI o del certificado de firma centralizada, 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 concurran 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 o revelación de las claves de acceso que permite la activación de la clave privada de firma centralizada, 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.
- Cese en la actividad del prestador de servicios de confianza salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos sean transferidos a otro prestador de servicios de confianza.
- 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.
- Así como las indicadas en la normativa de aplicación.

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. En caso de revocaciones masivas de oficio se notificara a los afectados a través de la correspondiente página web o, en su caso, en el Boletín Oficial del Estado. Asimismo, se podrá proceder a la generación de nuevos certificados siempre que se garantice la seguridad técnica y, en su caso, criptográfica de los procesos que sustentan. Por último, se notificará al organismo supervisor y, en caso pertinente, a otros organismos relevantes conforme a la normativa de aplicación.
- Se pone en conocimiento del ciudadano que todos los procedimientos relacionados con los documentos de identidad objeto de esta DPC, que implican el cambio del soporte físico van acompañados de la revocación de los certificados que contienen o que derivan de 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.

En cualquier caso, el prestador informará al firmante acerca de la revocación del certificado de manera previa o simultánea a la extinción, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

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 DNI, así como del robo o extravío de las claves de acceso a la clave privada de firma centralizada, o de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.
- El sistema permitirá al ciudadano la revocación voluntaria de su certificado de firma centralizada.

4.9.3 Procedimiento de solicitud de revocación

En el ámbito del DNI, las solicitudes de revocación se realizarán personalmente por el interesado ante cualquier equipo expedidor del DNI.

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 perdida, 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.

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 DNI podrá solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del firmante, o cualquier otro hecho que recomendará emprender dicha acción. En caso de revocaciones masivas de oficio se notificara a los afectados a través de la correspondiente página web o, en su caso, en el Boletín Oficial del Estado. Asimismo, se podrá proceder a la generación de nuevos certificados siempre que se garantice la seguridad técnica y, en su caso, criptográfica de los procesos que sustentan. Por último, se notificará al organismo supervisor y, en caso pertinente, a otros organismos relevantes conforme a la normativa de aplicación.

Por otro lado, en el ámbito del certificado de firma centralizada, para llevar a cabo este proceso, el ciudadano debe acceder con su usuario y contraseña al servicio de revocación del sistema Cl@ve y confirmar la operación mediante un segundo factor de autenticación. También podrá ejercer su derecho de revocación accediendo con su DNI o con cualquier otro certificado cualificado, así como de forma presencial en cualquier oficina de registro.

La revocación debe constatarse documentalmente, por lo que en cualquiera de estos procedimientos el ciudadano debe firmar la solicitud de revocación, ya sea con un certificado electrónico cualificado (incluido su certificado de firma electrónica centralizado antes de ser revocado) o de forma manuscrita.

Una vez revocado un certificado, el sistema garantiza que no se podrá utilizar en ningún caso durante un proceso de firma e informará al usuario de la revocación, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

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.

Por otro lado, el máximo retraso entre la confirmación de revocación de un certificado, o su suspensión, para ser efectivo y el cambio actual del estado de información del certificado será disponible a las partes de confianza, y que será como máximo de 60 minutos.

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

La solicitud de revocación de un certificado de firma cualificada 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 y firma electrónica así como de firma centralizada. 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 DNI y de los certificados de firma centralizada 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.

Se 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 mínimo de 4 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 DNI y los certificados de firma centralizada se dispone de varios prestadores de Servicios de Validación que proporcionan información sobre el estado de los certificados emitidos por la correspondiente jerarquía de certificación. Se trata de un servicio de validación en línea (Autoridad de Validación, AV) que implementa el "Online Certificate Status Protocol" siguiendo la RFC 6960. 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 6960.

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 DNI es un dispositivo cualificado de creación de firma electrónica certificado EAL4+ aumentado con AVA_VAN.5. 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.

Por otro lado, en el ámbito del certificado de firma centralizada, la clave privada que se genera quedará custodiada por la DGP, teniendo en cuenta que el acceso a esta clave será realizada por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del ciudadano.

En este sentido, el acceso a dicha clave sólo puede ser efectuado por el titular de la misma mediante Cl@ve permanente siendo necesario introducir un código de usuario (DNI/NIE), una contraseña tan sólo conocida por el ciudadano, y no almacenada en los sistemas de DGP, y un segundo factor de autenticación.

Por otro lado, desde DGP se replica la información necesaria para la autenticación y firma por parte del ciudadano hacia la Gerencia de Informática de la Seguridad Social (GISS), con objeto de crear una copia de seguridad y garantizar la continuidad del servicio.

En este sentido, se remite al contenido del apartado a) del artículo 18 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica a la espera de lo contemplado en la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

En línea con la mención anterior, en el apartado cuarto del anexo II del Reglamento (UE) 910/2014 se establece que, sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

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 DE LA DGP

5.1 CONTROLES FÍSICOS

Los aspectos referentes a los controles de seguridad física se encuentran recogidos en detalle en la documentación que la autoridad competente 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 DNI y de los certificados de firma centralizada 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 DNI y de los certificados de firma centralizada 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 DNI y de los certificados de firma centralizada 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 DNI y de los certificados de firma centralizada estarán físicamente separados de otros sistemas 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 DNI y de los certificados de firma centralizada 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 DNI y de los certificados de firma centralizada 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

En su caso, la autoridad competente ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

En su caso, la autoridad competente ha dispuesto planes de copia de respaldo, los mismos que para el resto de los sistemas de información, 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

En su caso, la autoridad competente 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.

La autoridad competente 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:

- **Responsable del Sistema**: También de la explotación de la Infraestructura de Clave Pública de la Dirección General de la Policía, es la persona responsable de la definición, desarrollo, operación y mantenimiento del Sistema durante todo su ciclo de vida, de verificar su correcto funcionamiento y que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- **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.
- **Auditores de Sistema**: Autorizados a consultar archivos, trazas y registros (logs) de auditoria de las entidades de la PKI y de los sistemas utilizados para la prestación de los Servicios de Confianza.
- **Responsables 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 de los sistemas de la Infraestructura de Clave Pública (PKI).

- **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 del DNI y de los certificados de firma centralizada se identifican mediante certificados electrónicos emitidos por la propia infraestructura 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 DNI y de los certificados de firma centralizada.

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 (Responsables 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 del DNI y de los certificados de firma centralizada deberá poseer el conocimiento, experiencia y formación suficientes, para el mejor cometido de las funciones asignadas.

Para ello, la autoridad competente 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 autoridad competente.

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 autoridad competente.

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 DNI y de los certificados de firma centralizada de forma inmediata al conocimiento del hecho.

5.3.7 Requisitos de contratación de terceros

Se aplicará la normativa general de la autoridad competente 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 firmante.
- 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 autoridad competente.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Responsable de Seguridad y el Administrador de Auditorías de DNI y de los certificados de firma centralizada. 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 autoridad competente 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 DNI y de los certificados de firma centralizada.

Los procedimientos de control de seguridad empleados en DNI y los certificados de firma centralizada 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 información 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 autoridad competente. Estos análisis deberían ser ejecutados, al menos, con periodicidad trimestral.

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 utilizada en la expedición de los certificados del DNI electrónico y firma centralizada conserva toda la información relevante sobre las operaciones realizadas con los certificados y se mantiene un registro de eventos.

Las operaciones registradas incluyen las realizadas por los administradores que utilizan las aplicaciones de administración de los elementos de DNI y los certificados de firma centralizada, 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, los Responsables de Seguridad y el Administrador de Auditorías de DNI y de los certificados de firma centralizada. 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 autoridad competente.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de información empleados por DNI y los certificados de firma centralizada 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 DNI y los certificados de firma centralizada 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 autoridad competente.

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 o 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 DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

La autoridad competente 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 confianza prestados por DNI y los certificados de firma centralizada.

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 creación de firma de alguna Autoridad de Certificación, el prestador informará a todos los titulares de certificados de DNI, los certificados de firma centralizada 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 DNI y de los certificados de firma centralizada 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 o del Boletín Oficial del Estado (ver apartado 2.1).

Las Autoridades componentes de DNI y de los certificados de firma centralizada dependientes de la AC afectada serán informadas del hecho y conminadas a solicitar una nueva certificación por otra AC del dominio de certificación.

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 DNI y de los certificados de firma centralizada cuenta con elementos redundantes y distintos centros. No obstante, el sistema de Autoridades de Certificación de DNI y de los certificados de firma centralizada 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 DNI y de los certificados de firma centralizada.
- 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

El prestador cualificado de servicio de confianza, DGP, contará con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i) tal como establece la letra i) del punto 2 artículo 24 del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

El procedimiento de cese efectivo de la actividad por parte del prestador cualificado será el indicado a continuación, a la espera de lo contemplado en la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

En el caso de que el prestador de servicios de confianza cese su actividad se comunicará a los firmantes que utilicen los certificados electrónicos que haya expedido; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de confianza que los asuma o, en caso contrario, extinguir su vigencia.

La citada comunicación se llevará a cabo a través del sitio web habilitado a tal efecto o del Boletín Oficial del Estado con un plazo mínimo de antelación de 2 meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador de servicios de confianza al que se propone la transferencia de la gestión de los certificados.

La Dirección General de la Policía comunicará al correspondiente Ministerio, 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.

La Dirección General de la Policía remitirá al correspondiente Ministerio 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 59/2003, de 19 de diciembre, de Firma electrónica. Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un periodo que considere suficiente en función de las consultas efectuadas al mismo.

5.8.2 Autoridad de Registro

No procede.

6. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES DE LA GISS

6.1 CONTROLES FÍSICOS

6.1.1 Ubicación física y construcción

El CPD de la GISS acoge la infraestructura de almacenamiento de la réplica de los certificados de firma centralizada. Este CPD es de uso exclusivo de la Gerencia Informática de la Seguridad Social.

El recinto consta de los siguientes sistemas de control de acceso físico:

- **Perímetro con valla de seguridad,** en cuya entrada hay una garita con vigilantes que controlan la entrada y salida de personas y vehículos.
- **Sistema de video-vigilancia,** tanto de las zonas exteriores como de las zonas comunes interiores.
- **Control de entrada al edificio con vigilantes armados,** tornos con acceso mediante tarjeta, arco de detección de metales y escáner para objetos.

Por otro lado, las instalaciones del CPD situado en la primera planta del edificio, disponen de las siguientes medidas:

- Controles de acceso físico.

- Protección ante desastres naturales.
- Medidas de protección ante incendios.
- Medidas ante fallos de los sistemas de soporte (energía eléctrica, telecomunicaciones, etc.).
- Protección contra el derribo de la estructura.
- Protección frente a inundaciones.
- Protección antirrobo.
- Recuperación ante un desastre.
- Controles para impedir la salida no autorizada de equipamientos, informaciones, soportes y aplicaciones, entre ellos las relativas a componentes utilizados para los servicios relacionados con los Certificados de firma centralizada objeto de le esta DPC.

Todas las operaciones críticas de los certificados de firma centralizada 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 de la semana. Estos sistemas están aislados de otros de la GISS, de forma que sólo el personal autorizado pueda acceder a ellos.

6.1.2 Acceso físico

En la entrada al CPD, el personal de la GISS pasa siempre a través de tornos que se abren mediante una tarjeta de control de acceso. Los vigilantes controlan los objetos que porten que deben pasar por escáner.

Una vez traspasado el control de entrada, el personal de la GISS debe ir identificado en todo momento con su tarjeta de acceso.

En el CPD se encuentran los sistemas informáticos principales que soportan la actividad de la organización y los principales procesos de las Entidades Gestoras y Servicios Comunes. Entre éstos hay sistemas mainframe, servidores, robots de cintas y sistemas de comunicaciones.

El CPD tiene un sistema de control de entrada mediante tarjeta inteligente, habilitado únicamente a determinado personal autorizado dentro de las instalaciones. Todos los accesos al CPD quedan registrados con la identificación de la persona que accede y la hora de entrada y de salida.

Las estancias del CPD están separadas por mamparas acristaladas que permiten el control visual.

Los sistemas que almacenan la réplica de los certificados de firma centralizada están físicamente aislados de otros sistemas 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 controladas por vigilantes, y se tiene que tener autorización previa para poder acceder a ellas.

Junto al muelle de entrada de equipos, hay unas oficinas donde se registran las entradas y salidas de los equipos. Todo el material que entra en las instalaciones debe pasar por un sistema que detecta si los equipos contienen sustancias peligrosas como explosivos.

6.1.3 Alimentación eléctrica y aire acondicionado

Los equipos informáticos donde se ubican los equipos de la infraestructura de firma centralizada y de almacenamiento de los certificados de firma centralizada están

convenientemente protegidos ante fluctuaciones o cortes de suministro eléctrico que puedan dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como uno de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

El sistema eléctrico que alimenta las maquinas del CPD esta redundado, existiendo dos tomas de entrada de energía que proceden de dos subcentrales diferentes.

Los equipos informáticos están ubicados en un entorno donde se garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

6.1.4 Exposición al agua

Existen las medidas de detección adecuadas para prevenir la exposición al agua de los equipos y el cableado que albergan la Infraestructura.

En el suelo técnico del CPD hay sensores de humedad para detectar inundaciones. Los sistemas de detección de agua están interconectados a través de un sistema informático que dispara una alarma si fuera necesario.

6.1.5 Protección y prevención de incendios

Todas las salas donde se ubican los activos de la infraestructura cuentan con sistemas automáticos de detección y extinción de incendios.

Por otro lado, existe un sistema de detección de incendios monitorizados desde la sala de control.

Así mismo, existen en el edificio extintores en las paredes de todas las salas y pasillos. Dichos extintores son revisados periódicamente de acuerdo a la normativa vigente.

6.1.6 Sistema de almacenamiento

El almacenaje en soportes de información se realiza de forma que se garantice tanto su integridad como su confidencialidad y cumpliendo los requisitos establecidos por la legislación vigente.

Se cuenta para ello con dependencias o armarios ignífugos y robots automatizados de tratamiento de cintas.

El acceso a estos soportes está restringido a personal autorizado.

6.1.7 Eliminación de los soportes de información

La eliminación de soportes se realiza mediante un contrato con una empresa que garantiza el cumpliendo de los requisitos establecidos por la legislación vigente.

6.1.8 Copias de seguridad fuera de las instalaciones

La Gerencia de Informática de la Seguridad Social (GISS) cuenta con un centro de respaldo para almacenar las copias de seguridad y garantizar la continuidad del servicio.

El CPD de respaldo reúne las mismas medidas de seguridad que el centro principal y dispone de la separación física adecuada.

Para garantizar la continuidad del servicio en caso de contingencia el Centro está comunicado con el CPD principal y los sistemas se encuentran replicados en tiempo real.

El CPD de respaldo dispone además de una sala acondicionada con puestos de trabajo para uso del personal en caso de contingencia.

6.2 CONTROLES DE PROCEDIMIENTO

Por otro lado, la GISS garantiza que sus sistemas se operan de forma segura, y por esto establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

El personal de operación de la infraestructura de firma centralizada realiza los procedimientos administrativos y de gestión de acuerdo con la política de seguridad establecida.

6.2.1 Roles responsables del control y gestión de la PKI

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

Se distinguen los siguientes perfiles:

- **Administradores de Sistema:** Usuarios autorizados para realizar las tareas relacionadas con la instalación, configuración y mantenimiento de los sistemas.
- **Responsable de seguridad:** Usuarios responsables de la definición, verificación, administración e implementación de las políticas, normas y procedimientos de seguridad.
- **Operadores de sistemas:** Serán los usuarios encargados de realizar las tareas básicas relativas a los sistemas involucrados en la infraestructura de firma centralizada, incluyendo los procesos de backup y recuperación.

6.2.2 Número de personas requeridas por tarea

Las funciones básicas de operación de la infraestructura de firma centralizada están soportadas por más de una persona, en grupos de trabajo activos y de respaldo, dentro de un plan que garantizan una disponibilidad inmediata en caso de contingencia grave en sus instalaciones.

6.2.3 Identificación y autenticación para cada usuario

Se han implantado unos estrictos sistemas de autenticación y autorización, de forma que el personal sólo accede a aquellos servicios que deba para realizar estrictamente sus funciones. De esta forma se preserva la integridad, confidencialidad y disponibilidad de la información manejada.

6.2.4 Roles que requieren segregación de funciones

Las prácticas de trabajo siguen el principio de que las tareas principales de administración y operación de los sistemas son realizadas por más de un trabajador, en ocasiones de departamentos diferentes, para minimizar el riesgo de actuaciones ilegítimas por parte de alguno de sus trabajadores.

6.3 CONTROLES DE PERSONAL

Se consideran los siguientes aspectos en cuanto a los controles de personal:

- Se mantiene confidencialidad de la información, asignando los medios necesarios y manteniendo una actitud adecuada en el desarrollo de sus funciones y, fuera del ámbito laboral, en aquello referente a la seguridad de las infraestructuras.

- Se es diligente y responsable en el tratamiento, mantenimiento y custodia de los activos de la infraestructura identificados en la política, en los planes de seguridad o en este documento.
- No se revela información no pública fuera del ámbito de la infraestructura, ni se extraen soportes de información a niveles de seguridad inferiores.
- Se utilizan los activos de la infraestructura para las finalidades que les han sido encomendadas.
- Se exige documentación escrita que marque sus funciones y medidas de seguridad a las que está sometido.
- El responsable de seguridad vela porque el punto anterior sea ejecutado, proporcionando a los responsables de área toda la información que fuera necesaria.
- No se instalan en ninguno de los sistemas de la infraestructura software o hardware que no sea expresamente autorizado por escrito por el responsable de sistemas de información.
- No se accede voluntariamente, ni se elimina o altera información no destinada a su persona o perfil profesional.

6.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Por otro lado, en relación a GISS, todo el personal que preste sus servicios en el ámbito del CPD de la Gerencia de Informática de la Seguridad Social debe superar un proceso de selección previo antes de tomar posesión de su puesto de trabajo, además de pertenecer a cuerpos especializados en el desarrollo y operación de los sistemas informáticos, así como en la gestión de proyectos.

El personal de empresas externas está clasificado por categorías profesionales y debe acreditar conocimientos o experiencia en las materias que debe dominar en sus puestos de trabajo.

6.3.2 Procedimientos de comprobación de antecedentes

Conforme a la normativa general de la Administración del Estado.

6.3.3 Requerimientos de formación

La GISS se responsabiliza de la formación al personal funcionario para asegurar la correcta realización de sus funciones de acuerdo con su rol y de solicitar formación para el personal externo para lograr la cualificación adecuada y saber responder ante situaciones de contingencia.

6.3.4 Requerimientos y frecuencia de actualización de la formación

Cuando es necesario se imparten cursos especializados, según los procedimientos que se establezca en la GISS.

6.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

6.3.6 Sanciones por actuaciones no autorizadas

Todo el personal que presta sus servicios en el ámbito de la infraestructura de firma centralizada está sometido a un régimen disciplinario en su condición de funcionario perteneciente a la administración pública.

Por otra parte, la GISS garantiza que se aplican cláusulas disciplinarias en los contratos de soporte técnico con las empresas externas, de manera que la responsabilidad del trabajador externo se transfiera a su empresa en caso de conducta punible.

6.3.7 Requisitos de contratación de terceros

La GISS contrata profesionales cualificados para la ejecución efectiva de las funciones propias.

El perfil del personal contratado está especificado en las cláusulas de los pliegos de contratación de las empresas.

6.3.8 Documentación proporcionada al personal

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

6.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

6.4.1 Tipos de eventos registrados

La GISS guarda registro de los eventos más significativos relacionados con la seguridad de la infraestructura de firma centralizada.

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 de intrusión física en las infraestructuras que dan soporte a la firma centralizada.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del firmante.
- 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 tendrán, como mínimo, la misma información que la descrita en el apartado 5.4.1 de la DPC.

6.4.2 Frecuencia de procesado de registros de auditoría

Los registros de auditoría se examinan cuando se considere necesario según las políticas de seguridad internas.

Se realizarán de forma periódica auditorías de control de los eventos registrados con una frecuencia al menos trimestral.

6.4.3 Periodo de conservación de los registros de auditoría

Los registros de auditoría se mantienen en línea durante al menos un año después de procesarlos y a partir de ese momento son archivados.

Una vez archivados, los registros de auditoría se conservarán, al menos, durante 15 años.

6.4.4 Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, se protegen de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

6.4.5 Procedimientos de respaldo de los registros de auditoría

Se generan diariamente copias de soporte incrementales del registro de auditoría y semanalmente copias completas.

6.4.6 Sistema de recogida de información de auditoría

El sistema interno de recopilación de información de auditoría está compuesto por los registros de la aplicación, los registros de red, los registros del sistema operativo, y además por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

6.4.7 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.

6.4.8 Análisis de vulnerabilidades

Los eventos en el proceso de auditoría son guardados para monitorizar las vulnerabilidades del sistema, entre otros motivos.

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

Estos análisis son ejecutados de acuerdo con su definición en el Plan de Auditoría.

6.5 ARCHIVO DE REGISTROS

La GISS garantiza que toda la información necesaria se guarda durante un periodo de tiempo apropiado.

6.5.1 Tipo de eventos archivados

La GISS conserva registrada por medios seguros toda la información y documentación relativa a la infraestructura de firma centralizada.

6.5.2 Periodo de conservación de registros

Toda la información y documentación relativa a la infraestructura de firma centralizada se conservará durante un mínimo de 15 años.

6.5.3 Protección del archivo

La GISS, en relación a los certificados de firma centralizada:

- Mantiene la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.
- Archiva los datos indicados anteriormente de forma completa y confidencial.
- Mantiene la privacidad de los datos de registro del ciudadano.

6.5.4 Procedimientos de copia de respaldo del archivo

La GISS realiza a diario copias incrementales de todos los datos que configuran la infraestructura de firma centralizada. Además, realiza copias de soporte completas, al menos una vez a la semana, para casos de recuperación de datos.

Los datos así recogidos se almacenan en un sistema de jerarquía de soportes de copias de seguridad que garantiza la integridad y la confidencialidad de las copias, así como la aplicación de una política predefinida de respaldo.

6.5.5 Requerimientos para el sellado de tiempo de los registros

La Autoridad de Sellado de Tiempo de la GISS garantiza el instante de tiempo en el que se realizan las principales actuaciones relacionadas con los sistemas de información empleados por la infraestructura de firma centralizada.

6.5.6 Sistema de archivo de información de auditoría

El sistema de archivo es interno dentro de la GISS. Además, la GISS tiene un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones.

6.5.7 Procedimientos para obtener y verificar información archivada

Solamente personas autorizadas por la GISS tienen acceso a los datos de archivo, sea en las mismas instalaciones de la GISS o en su ubicación externa.

Esta verificación debe ser llevada a cabo por los Auditores de Sistemas que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos.

6.6 RECUPERACIÓN EN CASOS DE VULNERACIÓN DE UNA CLAVE Y DE DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

6.6.1 Procedimientos de gestión de incidentes y vulnerabilidades

La GISS dispone de un Plan de Contingencias que establece los procedimientos que aplica en la gestión de las incidencias.

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.

6.6.2 Alteración de los recursos hardware, software y/o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos, la GISS iniciará las gestiones necesarias para hacer que el sistema vuelva a su estado normal de funcionamiento.

6.6.3 Instalación después de un desastre natural u otro tipo de catástrofe

La GISS desarrolla, mantiene, prueba y, si es necesario, ejecuta un Plan de Emergencia en caso de desastre, ya sea por causas naturales o intencionadas, sobre las instalaciones, que determina cómo se restauran los servicios de los sistemas de información.

La ubicación de los sistemas de recuperación de desastres dispone de las protecciones físicas de seguridad detalladas en la documentación del proyecto de Centro de Respaldo.

La GISS es capaz de restaurar la operación normal de la infraestructura de firma centralizada en las 24 horas siguientes al desastre, pudiendo, como mínimo, ejecutarse las siguientes acciones:

- Autenticación con Cl@ve Permanente.
- Firma centralizada con certificado de firma centralizada.

La base de datos de recuperación de desastres utilizada está sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el Plan de Seguridad. Los equipos de recuperación de desastres de la GISS tienen las medidas de seguridad físicas especificadas en el Plan de Seguridad.

7. CONTROLES DE SEGURIDAD TÉCNICA

La infraestructura del DNI y de los certificados de firma centralizada 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.

7.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

7.1.1 Generación del par de claves

Los pares de claves para los componentes internos de la PKI del DNI y de los certificados de firma centralizada, concretamente AC Raíz y ACs Subordinadas, se generan en módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de producto de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. Los sistemas de hardware y software que se emplean tienen en cuenta las normas europeas EN 419 261 y EN 419 221.

Las claves para los certificados de identidad y firma cualificada (DNI) emitidos por la AC *Subordinada* se generan en la propia tarjeta criptográfica del titular, la cual cumple los requisitos de Dispositivo Cualificado de Creación de Firma Electrónica (nivel de seguridad CC EAL4+ aumentado con AVA_VAN.5).

Las claves para los certificados de firma centralizada se generan en el dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalentes.

7.1.2 Entrega de la clave privada al titular

En el ámbito del DNI, 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.

Por otro lado, en el ámbito del certificado de firma centralizada, una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro, ha activado su Cl@ve Permanente, y ha solicitado expresamente la emisión de sus certificados de firma centralizada, dicha emisión se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma.

El sistema informará al ciudadano de que se le va a emitir su certificado de firma centralizada y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial.

7.1.3 Entrega de la clave pública al emisor del certificado

En el ámbito del DNI, 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 DNI formando parte de una solicitud de certificación en formato PKIX-CMP.

En el ámbito del certificado de firma centralizada la clave pública es enviada a la PKI del DNI formando parte de una solicitud de certificación en formato PKIX-CMP.

7.1.4 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 DNI y de los certificados de firma centralizada, 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 o en el Boletín oficial del Estado.

7.1.5 Tamaño de las claves

El tamaño de las claves de la AC Raíz y AC Raíz 2 es de 4096 bits.

El tamaño de las claves de las AC Subordinadas emitidas por AC Raíz es de 2048 bits.

El tamaño de las claves de las AC Subordinadas emitidas por AC Raíz 2 es de 4096 bits.

El tamaño de las claves de los certificados del *DNI* es de 2048/1920 bits [Ver nota informativa] *y de los certificados de firma centralizada* es de 2048 bits.

7.1.6 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 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

La clave pública de los certificados de *DNI y de los certificados de firma centralizada* está codificada de acuerdo con RFC 5280 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 la norma "Electronic Signatures and Infrastructures (ESI); "Cryptographic Suites" ETSI TS 119 312 y "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for cryptographic suites" ETSI TR 119 300, que indica la calidad de los algoritmos de firma electrónica. Los algoritmos y parámetros de firma utilizados por las Autoridades de Certificación del DNI y de los certificados de firma centralizada 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-256.

7.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3)

Los usos admitidos de la clave para cada tipo de certificado emitido por DNI y de los certificados de firma centralizada vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por DNI y certificados de firma centralizada 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 el prestador.

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, en el caso del DNI, y para la firma electrónica de ficheros y transacciones en el caso de los certificados de firma centralizada.

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

CERTIFICADO	KEY USAGE
Certificado de Firma (2.16.724.1.2.2.2.3)	contentCommitment[3]
Certificado de Autenticación (2.16.724.1.2.2.2.4)	Digital Signature

Mientras que en el caso de los certificados de firma centralizada se ha incluido el siguiente:

CERTIFICADO	KEY USAGE
Certificado de Firma (2.16.724.1.2.2.2.11)	contentCommitment

7.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

7.2.1 Estándares para los módulos criptográficos

Los módulos utilizados para la creación de claves utilizadas por AC Raíz y ACs *Subordinadas* de DNI y de los certificados de firma centralizada cumplen los requisitos establecidos en un perfil de protección de producto de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. Los sistemas de hardware y software que se emplean tienen en cuenta las normas europeas EN 419 261 y EN 419 221.

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 cualificados de creación de firma electrónica, cumplen el nivel de seguridad CC EAL4+ y soportan los estándares PKCS#11 y CSP.

7.2.2 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[4]. Ésta se activa mediante la inicialización del software de AC por medio de

[3] Nonrepudiation[4] 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.

[4] 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.

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

La clave privada de los Certificados de DNI está bajo el exclusivo control del ciudadano titular del DNI, así como la clave privada de los certificados de firma centralizada está, con un alto nivel de confianza, bajo el exclusivo control del ciudadano.

7.2.3 Custodia de la clave privada

Las claves privadas de las Autoridades de Certificación se encuentran alojadas en dispositivos criptográfico que cumplen los requisitos establecidos en un perfil de protección de producto de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

En el ámbito del DNI, la custodia de las claves privadas de los certificados de Identidad Pública y firma electrónica 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 DNI 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 DNI) 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.

Por otro lado, en el ámbito de los certificados de firma centralizada, la custodia de la clave privada la realiza la autoridad competente siendo únicamente los ciudadanos titulares de las mismas los que pueden acceder a dicha clave a través de Cl@ve permanente siendo necesario introducir un código de usuario (DNI/NIE), una contraseña tan sólo conocida por el ciudadano, y no almacenada en los sistemas de DGP, y un segundo factor de autenticación.

En todo momento el ciudadano podrá modificar la clave personal de acceso a través del sistema Cl@ve.

7.2.4 Copia de seguridad de la clave privada

Las claves privadas de las ACs 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 y firma electrónica ya que las claves no pueden ser exportadas de las tarjetas y éstas no son clonables.

Por otro lado, en el ámbito de los certificados de firma centralizada, la autoridad competente realiza copias de seguridad de las claves privadas protegidas, siendo éstas únicamente accesibles por el ciudadano.

Dichas copias de seguridad podrán estar albergadas en la GISS, con el fin de garantizar la continuidad de la prestación de los servicios de firma centralizada, que realiza junto con la DGP responsable último de la prestación segura de dicho servicio.

7.2.5 Archivo de la clave privada

Las claves privadas de la ACs 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 DNI 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.

Por otro lado, en el ámbito de los certificados de firma centralizada, la autoridad competente mantiene, según la legislación vigente, las copias de seguridad con las claves privadas protegidas, siendo éstas únicamente accesibles por el ciudadano.

7.2.6 Transferencia de la clave privada a o desde el módulo criptográfico

La transferencia de la clave privada de las ACs 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 DNI. La generación de claves y la importación de los certificados asociados sólo pueden realizarse desde un puesto autorizado de una Oficina de Expedición.

7.2.7 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 que hacen uso de dichos módulos.

La tarjetas soporte del DNI son dispositivos cualificados de creación de firma electrónica y cumplen el nivel de seguridad CC EAL4+ aumentado con AVA_VAN.5. 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.

En relación al certificado de firma centralizada, la clave privada asociada se utiliza en un dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalentes.

7.2.8 Método de activación de la clave privada

Tal y como se estipula en el apartado *7.2.2 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 DNI y que debe permanecer bajo su exclusivo conocimiento.

Por otro lado, la activación de la clave privada del certificado de firma centralizada requiere la introducción de Cl@ve permanente siendo necesario introducir un código de usuario (DNI/NIE), una contraseña tan sólo conocida por el ciudadano, y no almacenada en los sistemas de DGP, y un segundo factor de autenticación.

7.2.9 Método de desactivación de la clave privada

Un Administrador puede proceder a la desactivación de la clave de las Autoridades de Certificación 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 y firma electrónica se pueden desactivar retirando la tarjeta del lector o pasado el tiempo establecido tras la introducción de la clave personal de acceso.

Por otro lado, en el ámbito del certificado de firma centralizada, si un ciudadano autenticado en el sistema se equivoca repetidas veces en su contraseña de firma, tanto su clave como el certificado de firma se bloquearán automáticamente.

7.2.10 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 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 y firma electrónica 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 DNI asociada.
- Irá acompañada de la inutilización física de la tarjeta que la alberga, cuando se renueve el DNI (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.

Por otro lado, en el ámbito del certificado de firma centralizada en procesos de renovación/revocación se destruyen las claves de los ciudadanos. El certificado es revocado por la DGP, y las claves y certificados dados de baja de forma segura incluyendo las copias realizadas para garantizar la continuidad del servicio.

7.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

7.3.1 Archivo de la clave pública

La Infraestructura de Clave Pública del DNI y de los certificados de firma centralizada, en cumplimiento de lo establecido por el artículo 20.1 f) de la LFE 59/2003 (en conformidad con el artículo 24.2 h) del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza) 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.

7.3.2 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 tienen una validez de treinta (30) años y los de la AC Subordinada 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 confianza.

El periodo máximo de validez de los Certificados de Identidad Pública y firma electrónica es hasta 60 meses [Ver nota informativa], mientras que los certificados de firma centralizada tienen una caducidad máxima de 60 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, firma electrónica y firma centralizada superarán la fecha de caducidad impresa del soporte físico de los documentos referidos en el punto 1.3.7 de esta DPC.

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: 2, 5, 10 años y permanente. La renovación de los Certificados sobre una misma tarjeta se deberá realizar, en la situación más habitual, 1 y 2 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 DNI 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 59/2003, de 19 de diciembre, de Firma Electrónica así como el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza) la renovación a través de los Puntos de Actualización del DNI 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 del DNI y los certificados de firma centralizada, originando el cese permanente de su operatividad conforme a los usos que le son propios.

La caducidad de un Certificado de Identidad Pública y firma electrónica así como del certificado de firma centralizada inhabilita el uso legítimo por parte del Ciudadano.

7.4 DATOS DE ACTIVACIÓN

7.4.1 Generación e instalación de los datos de activación

Para la instauración de una Autoridad de Certificación del dominio del DNI y de los certificados de firma centralizada 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.

Para realizar firma centralizada, se necesita como modalidad de identificación utilizar Cl@ve permanente siendo necesario introducir un código de usuario (DNI/NIE), una contraseña tan sólo conocida por el ciudadano, y no almacenada en los sistemas de DGP y de la GISS, y un segundo factor de autenticación.

El acceso a los certificados está protegido por Cl@ve permanente, por lo que para poder usar la firma centralizada será necesario activar la misma.

7.4.2 Protección de los datos de activación

Sólo el personal autorizado, en este caso los Operadores y Administradores de la PKI del DNI y de los certificados de firma centralizada 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 los claves asociadas a los certificados de Identidad Pública y firma electrónica 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.

En el caso de la clave asociada al certificado de firma centralizada del ciudadano, sólo éste conoce la contraseña personal introducida al generar la Cl@ve permanente y un segundo factor de autenticación, siendo por tanto el único responsable de la protección de los datos de activación de su clave privada.

Tanto la clave personal de acceso (PIN) como la clave de acceso a la clave privada del certificado de firma centralizada son confidenciales, personales e intransferibles 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:

- Memorícelas y procure no anotarlas en ningún documento físico ni electrónico que el Titular conserve.
- No envíe ni comunique a nadie ni por ningún medio, ya sea vía telefónica, correo electrónico, etc.

- Recuerde que son personales e intransferibles. Si cree que esta información puede ser conocida por otra persona, debe cambiarla. El uso de las mismas por persona distinta del Titular presupone grave negligencia por parte del mismo y permite la activación de las claves privadas para poder realizar operaciones de firma electrónica en su nombre. Es obligación del titular notificar la pérdida de control sobre su clave privada, a causa del compromiso de las mismas, ya que es motivo de revocación del certificado asociado a dichas claves.
- Como medida adicional, deberá abstenerse de escoger un número relacionado con sus datos personales, así como cualquier otro código que pueda resultar fácilmente predecible por terceras personas (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones de la misma cifra, secuencias de cifras que ya forman parte de su número de DNI, etc.)
- Se recomienda cambiarlo periódicamente.

7.4.3 Otros aspectos de los datos de activación

En el caso de las claves asociadas a los certificados de Identidad Pública y firma así como el certificado de firma centralizada del ciudadano, éste podrá modificar de forma telemática los datos de activación siempre que permanezcan bajo su conocimiento, esto es, no hayan sido olvidados o se haya bloqueado debido a intentos de acceso fallidos con datos de activación incorrectos.

En el ámbito del DNI, el ciudadano podrá modificar la clave personal de acceso –PIN- en los Puntos de Actualización del DNI 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.

7.5 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.

7.5.1 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 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

7.5.2 Evaluación de la seguridad informática

Los procesos de gestión de la seguridad de la infraestructura soporte del DNI y de los certificados de firma centralizada 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 DNI son fiables, facilitando el cumplimiento de las recomendaciones de seguridad para sistemas de gestión de certificados digitales para firmas electrónicas (EN 419 261), evaluándose el grado de cumplimiento mediante un perfil de protección adecuado, 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 DNI y de los certificados de firma centralizada*.

7.6 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.

7.6.1 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 DNI y los certificados de firma centralizada.

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 DNI y de los certificados de firma centralizada, 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 DNI y de los certificados de firma centralizada está dotada de entornos de desarrollo, preproducción y producción claramente diferenciados e independientes.

7.6.2 Controles de gestión de seguridad

La organización encargada del sistema del DNI y de los certificados de firma centralizada, 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.

7.6.3 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 DNI y de los certificados de firma centralizada.

7.7 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 DNI y los certificados de firma centralizada 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.

7.8 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, aspecto que posteriormente ha sido recogido por la Ley 32/2014, de 22 de diciembre, de Metrología.

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

Por otro lado, el tiempo utilizado para la prestación de los servicios de revocación estará sincronizada con UTC al menos una vez cada 24 horas.

8. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

8.1 PERFIL DE CERTIFICADO

Los certificados de DNI y de firma centralizada tendrán en cuenta las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, May 2008.
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework.
- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la EN).

8.1.1 Número de versión

Los certificados de DNI y de firma centralizada emitidos por la AC Subordinada utilizan el estándar X.509 versión 3 (X.509 v3).

8.1.2 Extensiones del certificado

Los Certificados de DNI y de firma centralizada 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, toda esta información estará firmada electrónicamente por el prestador encargado de la emisión de los certificados.

Los datos personales del Ciudadano incluidos en los certificados 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.
- Dirección de correo (opcional para DNI)

Las extensiones utilizadas en los certificados son:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *Subject Alternative Names (dirección de correo del titular del certificado para DNI)*
- *Auth. Information Access*
- *Biometricinfo (para DNI)*
- *Subject Directory Attributes*
- *qcstatements*

Los certificados tienen 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 comienzan con el prefijo 2.16.724.1.2.2.3.

El DNI tiene definidas las siguientes extensiones propietarias:

OID	Concepto	Descripción
2.16.724.1.2.2.4.1	PersonalDataInfo	Hash de los datos biográficos (datos impresos en el DNI)

A continuación se recogen los perfiles de los tipos de certificados que se emiten para DNI y Firma Centralizada por la Raíz 1 y 2 del DNI.

Certificado de Firma de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	SHA256withRSAEncryption	
4. Issuer Distinguished Name	CN=AC DNIE XXX [5] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	Máximo 60 meses [Ver nota informativa]	
6. Subject	CN=APELLIDO1 APELLIDO2, NOMBRE (FIRMA) G=NOMBRE SN=APELLIDO1 NÚMERO DE SERIE=DNI (con letra)	

[5] XXX es un número de tres dígitos que identifica a la AC emisora

Certificado de Firma de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
	C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048/ 1920 bits [Ver nota informativa]	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
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	0	
ContentCommitment	1	
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	2.16.724.1.2.2.2.3	
URL DPC	http://pki.policia.es/dnie/publicaciones/dpc (Raíz 2) http://www.dnie.es/dpc (Raíz 1)	
Notice Reference	DIRECCIÓN GENERAL DE LA POLICÍA, VATES-S2816015H	
7.Policy Mappings		
8. Subject Alternative Names	email del titular	NO
9. Issuer Alternative 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: http://ocsp.dnie.es CA: http://www.dnie.es/certs/AC00X.crt[6] (Raíz 1)	NO

[6] X = 1, 2 ó 3

Certificado de Firma de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
	CA: http://pki.policia.es/dnie/certs/AC00X.crt[7] (Raíz 2)	
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 (2.16.724.1.2.2.4.1)	Hash de los datos biográficos (datos impresos en el DNI) SHA1/SHA256	
21. qcstatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcType : (esign) id-etsi-qcs-QcPDS : (https://www.dnie.es/pds) (Raíz 1) y (https://pki.policia.es/dnie/publicaciones/pds) (Raíz 2) id-etsi-qcs-QcRetentionPeriod : (15 años)	

[7] X = 4, 5 ó 6

Certificado de Autenticación de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	SHA256withRSAEncryption	
4. Issuer Distinguished Name	CN=AC DNIE XXX[8] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	Máximo 60 meses [Ver nota informativa]	
6. Subject	CN=APELLIDO1 APELLIDO2, NOMBRE (AUTENTICACIÓN) G=NOMBRE SN=APELLIDO1 NÚMERO DE SERIE=DNI (con letra) C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048/ 1920 bits [Ver nota informativa]	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
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	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	http://pki.policia.es/dnie/publicaciones/dpc (Raíz 2) http://www.dnie.es/dpc (Raíz 1)	

[8] XXX es un número de tres dígitos que identifica a la AC emisora

Certificado de Autenticación de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Notice Reference	DIRECCIÓN GENERAL DE LA POLICÍA, VATES-S2816015H	
7.Policy Mappings		
8. Subject Alternative Names	email del titular	NO
9. Issuer Alternative 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: http://ocsp.dnie.es CA: http://www.dnie.es/certs/AC00X.crt[9] (Raíz 1) CA: http://pki.policia.es/dnie/certs/AC00X.crt[10] (Raíz 2)	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 (2.16.724.1.2.2.4.1)	Hash de los datos biográficos (datos impresos en el DNI) SHA1/SHA256	

Por otro lado, se recoge el perfil del tipo de certificado de firma centralizada.

Certificado de firma centralizada de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	SHA256withRSAEncryption	

[9] X = 1, 2 ó 3

[10] X = 4, 5 ó 6

Certificado de firma centralizada de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
4. Issuer Distinguished Name	CN=AC DNIE XXX [11] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	Máximo 60 meses	
6. Subject	CN=APELLIDO1 APELLIDO2, NOMBRE (FIRMA CENTRALIZADA) G=NOMBRE SN=APELLIDO1 NÚMERO DE SERIE=DNI (con letra) | NIE (con letra) C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048 bits	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
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	0	
ContentCommitment	1	
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	2.16.724.1.2.2.2.11	
URL DPC	http://www.dnie.es/dpc (Raíz 1) http://pki.policia.es/dnie/publicaciones/dpc (Raíz 2)	
Notice Reference	DIRECCIÓN GENERAL DE LA POLICÍA, VATES-S2816015H	
7.Policy Mappings		
8. Subject Alternative Names	No se utilizará	NO
9. Issuer Alternative Names	No se utilizará	
10. Subject Directory	DateOfBirth	

[11] XXX es un número de tres dígitos que identifica a la AC emisora

Certificado de firma centralizada de Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Attributes	countryOfCitizenship	
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: http://ocsp.dnie.es CA: http://www.dnie.es/certs/AC00X.crt[12] (Raíz 1) CA: http://pki.policia.es/dnie/certs/AC00X.crt[13] (Raíz 2)	NO
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. Biometricinfo	No se utilizará	NO
20. personalDataInfo (2.16.724.1.2.2.4.1)	No se utilizará	
21. qcstatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcType : (esign) id-etsi-qcs-QcPDS : (https://www.dnie.es/pds) (Raíz 1) y (https://pki.policia.es/dnie/publicaciones/pds) (Raíz 2) id-etsi-qcs-QcRetentionPeriod : (15 años)	

Los certificados DNI y de firma centralizada se emiten en calidad de certificados cualificados y, por tanto ambos perfiles contienen los campos que establece la normativa legalmente aplicable en materia de Certificados Cualificados.

8.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

8.1.4 Formatos de nombres

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

[12] X = 1, 2 ó 3

[13] X = 4, 5 ó 6

8.1.5 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 (Givename), SN (Surname) y serialNumber del DN serán los que distingan a los DN entre sí. La sintaxis de estos atributos es la siguiente:

CN= Apellido1 Apellido2, Nombre (AUTENTICACIÓN|FIRMA|FIRMA CENTRALIZADA)

GN = Nombre

SN = Apellido1

SerialNumber= NNNNNNNNA (número de DNI con letra | NIE con letra)

8.1.6 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 son los siguientes:

Política de Certificados Cualificados de Autenticación	2.16.724.1.2.2.2.4
Política de Certificados Cualificados de Firma Electrónica	2.16.724.1.2.2.2.3
Política de Certificados Cualificados de Firma centralizada	2.16.724.1.2.2.2.11

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.

8.1.7 Uso de la extensión "PolicyConstraints"

No estipulado.

8.1.8 Sintaxis y semántica de los "PolicyQualifier"

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

- URL DPC: contiene la URL donde se 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.

8.1.9 Tratamiento semántico para la extensión "Certificate Policy"

Teniendo en cuenta los matices introducidos por la rfc5280 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 DNI y de certificados de firma centralizada). En los certificados de ciudadano se incluirían respectivamente los identificadores de política para autenticación (2.16.724.1.2.2.2.4), firma (2.16.724.1.2.2.2.3) y firma centralizada (2.16.724.1.2.2.2.11) recogidos en esta DPC.

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

8.2 PERFIL DE CRL

8.2.1 Número de versión

La infraestructura del DNI y de certificados de firma centralizada soporta y utiliza CRLs X.509 versión 2 (v2).

8.2.2 CRL y extensiones

Las CRLs emitidas por el sistema del DNI y de certificados de firma centralizada serán conformes con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, May 2008
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework

8.3 PERFIL DE OCSP

8.3.1 Perfil del certificado OCSP responder

Los certificados de OCSP responder serán emitidos por una de las AC subordinadas del dominio de certificación del DNI y de certificados de firma centralizada, siendo conformes con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, May 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- IETF RFC 6960 Online Certificate Status Protocol – **OCSP**

El periodo de validez de los mismos será no superior a 6 meses. Tal y como contempla la rfc 6960, 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.

8.3.2 Número de versión

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

8.3.3 Formatos de nombres

Los certificados de OCSP Responder emitidos por una AC del dominio del DNI y de certificados de firma centralizada 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= OCSP Responder DNIE XXX

OU=<DATOS PRESTADOR VALIDACION>

OU=DNIE

O=DIRECCION GENERAL DE LA POLICIA

C=ES

8.3.4 Identificador de objeto (OID) de la Política de Certificación

El identificador de la Política de Certificación bajo la que se emite los certificados de OCSP Responder del DNI y de certificados de firma centralizada es el siguiente:

Política de Certificados de OCSP Responder	2.16.724.1.2.2.2.5

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

8.3.5 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

A continuación se recoge el perfil del certificado de OCSP Responder que emite la infraestructura de clave pública del DNI y de certificados de firma centralizada.

Certificado de OCSP responder Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	SHA256withRSAEncryption	
4. Issuer Distinguished Name	CN=AC DNIE XXX [14] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	6 meses	
6. Subject	CN= OCSP Responder DNIE XXX OU=<DATOS PRESTADOR VALIDACION> OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048 bits	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
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	

[14] XXX es un número de tres dígitos que identifica a la AC emisora

Certificado de OCSP responder Ciudadano		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
ContentCommitment	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
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	http://www.dnie.es/dpc (Raíz 1) http://pki.policia.es/dnie/publicaciones/dpc (Raíz 2)	
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. OCSPNoCheck	Valor NULL como contempla la norma	NO

Certificado de OCSP responder AC Subordinadas		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	SHA256withRSAEncryption	
4. Issuer Distinguished Name	CN=AC RAIZ DNIE X [15] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	

[15] X es un número que identifica a la AC emisora

Certificado de OCSP responder AC Subordinadas		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
5. Validez	6 meses	
6. Subject	CN= AV DNIE <ID PRESTADOR VALIDACION> OU=<DATOS PRESTADOR VALIDACION> OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048 bits	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
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	0	
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	http://www.dnie.es/dpc (Raíz 1) http://pki.policia.es/dnie/publicaciones/dpc (Raíz 2)	
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. OCSPNoCheck	Valor NULL como contempla la norma	NO

8.3.6 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 rfc6960.

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

8.3.7 Formato de las respuestas

El OCSP responder de los prestadores de servicios de validación del DNI y de firma centralizada 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 DNI y de los certificados de firma centralizada, y que consten en las CRLs.
- "Good", para aquellos certificados emitidos por las AC del dominio de certificación del DNI y de los certificados de firma centralizada, 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 rfc6960 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.

La información del estado de revocación se hará disponible más allá del periodo de validez del certificado durante el periodo de tiempo establecido por la normativa en vigor. En este sentido, el respondedor OCSP debería utilizar la extensión "ArchiveCutOff" con la fecha y hora del inicio de validez del certificado de la AC, tal como se especifica en IETF RFC 6960.

8.3.8 Fechado de 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.

9. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

9.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Se llevará a cabo una auditoría sobre el sistema del DNI y de certificados de firma centralizada de forma anual en conformidad con EN 319 411-2, de acuerdo con el Plan de Auditorías de la Autoridad Competente. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta DPC.

Por otro lado, el Plan de Auditorías podrá contemplar el desarrollo de auditorías internas a las Autoridades de Registro en conformidad con EN 319 411-1 y el Reglamento 910/2014.

Sin perjuicio de lo anterior, que la Autoridad Competente 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.

También, se establecerán controles periódicos en materia de protección de datos de carácter personal.

Por último, el prestador cualificado de servicios de confianza será auditado, al menos cada 24 meses por un organismo de evaluación de la conformidad según se establece en el Reglamento 910/2014.

9.2 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 DNI y de certificados de firma centralizada 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 DNI y de certificados de firma centralizada.
- En general los criterios establecidos en norma europea EN 319 403.

9.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Al margen de la función de auditoría, el auditor externo y la parte auditada 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.

9.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría determinará la adecuación de los servicios de DNI y de los certificados de firma centralizada 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 las normas europeas EN 319 411-2, EN 319 411-1 y EN 319 401.

9.5 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.

9.6 COMUNICACIÓN DE RESULTADOS

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

10. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

10.1 TARIFAS

10.1.1 Tarifas de emisión de certificado o renovación

No aplica en el ámbito de los certificados de firma centralizada.

Respecto al DNI, la expedición 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.

10.1.2 Tarifas de acceso a los certificados

No aplica.

10.1.3 Tarifas de acceso a la información de estado o revocación

No aplica.

10.1.4 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.

10.1.5 Política de reembolso

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

10.2 RESPONSABILIDADES ECONÓMICAS

Subsumido en el apartado 10.8.

10.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

10.3.1 Ámbito de la información confidencial

Toda información que no sea considerada por la Autoridad Competente 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 DNI y de los certificados de firma centralizada:

  Para garantizar la confidencialidad de las claves privadas, de autenticación y firma, la Autoridad de Registro, proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro en presencia del ciudadano y de un funcionario habilitado a tal efecto. En el ámbito del DNI, dichas claves serán entregadas al ciudadano grabadas en el procesador de su 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.

  En el ámbito del certificado de firma centralizada la confidencialidad de las claves privadas no será necesaria para su generación la presencia de un funcionario siendo emitidos conforme al apartado 4.3.1 de esta DPC.

- Confidencialidad en la prestación de servicios de confianza:

  Se 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 DNI y de los certificados de firma centralizada tiene el deber de guardar secreto establecida legal o convencionalmente.
- Toda la información clasificada como "Confidencial".

10.3.2 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.
- Los términos y condiciones del servicio de confianza.
- La información sobre el estado de los certificados.
- Toda otra información identificada como "Pública".

10.3.3 Deber de secreto profesional

Todas las personas que participan en cualesquiera tareas propias o derivadas de la emisión y gestión del DNI y de los certificados de firma centralizada están obligadas 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 DNI y de los certificados de firma centralizada estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con la Institución del DNI.

10.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

10.4.1 Política de protección de datos de carácter personal

De acuerdo con la legislación española al respecto, se recoge dentro del capítulo 11, apartado 11.1 y siguientes.

10.4.2 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 (ver artículo 4.1 Reglamento general de protección de datos).

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 confianza 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 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal así como sometido al ámbito de aplicación de la Ley vigente en Protección de Datos.

10.4.3 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, 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.

10.4.4 Responsabilidad de la protección de los datos de carácter personal

Esta responsabilidad se regula en el capítulo 11.

10.4.5 Comunicación y consentimiento para usar datos de carácter personal

Se llevará a cabo en el procedimiento de primera inscripción, informando a los ciudadanos titulares de los certificados de la obtención de sus datos personales.

10.4.6 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.

10.4.7 Otras circunstancias de publicación de información

Estas posibles circunstancias se regulan en el capítulo 11.

10.5 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 DNI y los certificados de firma centralizada 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.

10.6 OBLIGACIONES

10.6.1 Obligaciones de la AC

La Autoridad de Certificación *Subordinada* de DNI y de los certificados de firma centralizada actuará relacionando una determinada clave pública con su titular a través de la emisión de un certificado de firma cualificada, 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 cualificada personales y la provisión del dispositivo cualificado de creación de firma electrónica.

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 10.12.2 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 del DNI y de firma centralizada 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 ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se aplicarán los procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el firmante controle de modo exclusivo el uso de sus datos de creación de firma.

Solo los prestadores de servicios de confianza que expidan certificados cualificados podrán gestionar los datos de creación de firma electrónica en nombre del firmante. Para ello, podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No podrán duplicar los datos de creación de firma para ninguna otra finalidad.

14º Colaborar con los procesos de auditoría.

15º Operar de acuerdo con la legislación aplicable.

16º El prestador cualificado de servicio de confianza, DGP, contará con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i) tal como establece la letra i) del punto 2 artículo 24 del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE tal como se recoge en el epígrafe 5.8.1.

17º Cuando el prestador de servicios gestione los datos de creación de firma en nombre del firmante, deberá custodiarlos y protegerlos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante.

Así como todas las contempladas en el artículo 24 del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

10.6.2 Obligaciones de la AR

Las Oficinas de Expedición del DNI y de los certificados de firma centralizada 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, en el caso de la expedición del DNI. No almacenando ni copiando los datos de creación de

firma de los certificados DNI o sin proteger siendo sólo accesibles por los titulares de los certificados de firma centralizada.

4º Tramitar las peticiones de revocación lo antes posible.

5º Notificación al ciudadano de la revocación 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 en conformidad con esta DPC.

6º Comprobar que toda la información incluida o incorporada por referencia en el certificado es exacta.

7º Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado 11.

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.

9º Las obligaciones de las entidades registradores establecidas en la Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones, por las que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

10.6.3 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 los términos y condiciones del servicio de confianza, 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 Autoridad Competente, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento del certificado.

5º Proteger sus claves privadas, así como claves de acceso 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 del DNI y de los certificados de firma centralizada.

9º Informar inmediatamente a la Autoridad Competente 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 confianza, sin permiso previo por escrito de la Autoridad de Certificación.

12º Cumplir las obligaciones que se establecen para los ciudadanos titulares de los certificados en este documento y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica así como el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

10.6.4 Obligaciones de los terceros aceptantes

A) Es obligación de los terceros que acepten y confíen en los certificados emitidos por DNI y de firma centralizada:

- 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 de 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 habilite a tal efecto.

B) Los prestadores de servicios 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 servicio otorguen a dichos certificados.
- En caso que el Prestador de Servicios consulte en línea el estado de un Certificado de DNI y de firma centralizada 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 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 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 dé 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 deberá conocer y aceptar toda restricción a que esté sujeto el citado Certificado.

10.6.5 Obligaciones de otros participantes

No estipulado

10.7 LIMITACIONES DE RESPONSABILIDAD

Subsumido en 10.8.

10.8 RESPONSABILIDADES

10.8.1 Limitaciones de responsabilidades

Las autoridades competentes que tienen atribuidas las competencias del DNI y de los certificados de firma centralizada responderán 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, en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza así como en la presente DPC.

En este sentido, el prestador de servicios de confianza 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 confianza.

10.8.2 Responsabilidades de la Autoridad de Certificación

- La Autoridad Competente 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, el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.
- La responsabilidad del prestador de servicios de confianza regulada en la 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 confianza demostrar que actuó con la diligencia profesional que le es exigible siendo responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento 910/2014.
- Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando el prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero del artículo 13 del Reglamento 910/2014 se produjeron sin intención ni negligencia por su parte.
- Cuando DGP, como prestador cualificado de servicios de confianza, informe debidamente a los ciudadanos con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

- De manera particular, la Dirección General de la Policía (Ministerio del Interior) como prestador de servicios de confianza 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 Dirección General de la Policía (Ministerio del Interior) como prestador de servicios de confianza 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 confianza.
- 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.
- 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 electrónico.
- 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 del DNI y los certificados de firma centralizada.
- 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.

10.8.3 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.

10.8.4 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. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al ciudadano.

El Documento Nacional de Identidad electrónico 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.

10.8.5 Delimitación de responsabilidades

Las ACs de DNI y de los certificados de firma centralizada 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.4	Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta DPC.
RESP.5	Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos.
RESP.6	Ocasionados por el mal uso de la información contenida en el certificado.
RESP.7	La AC no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se autentiquen mediante un certificado emitido por ella.

10.8.6 Alcance de la cobertura

En el artículo 24.2 c) del Reglamento 910/2014 se informa que c) con respecto al riesgo de la responsabilidad por daños y perjuicios de conformidad con el artículo 13, el prestador cualificado de servicios de confianza mantendrá recursos financieros suficientes u obtendrán pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional.

En este sentido, tanto la Ley 59/2003 de Firma Electrónica, como la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza exceptúa a la DGP de la constitución de garantía o seguro de responsabilidad civil.

10.8.7 Cobertura de seguro u otras garantías para los terceros aceptantes

Ver apartado anterior.

10.9 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.

10.10 PERIODO DE VALIDEZ

10.10.1 Plazo

Esta DPC entra en vigor desde el momento de su publicación.

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.

10.10.2 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, si bien se conservará durante 15 años.

10.10.3 Efectos de la finalización

Las obligaciones y restricciones que establece esta DPC, en referencia a auditorías, información confidencial, obligaciones y responsabilidades, nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

10.11 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 y los certificados de firma centralizada 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 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.

10.12 PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES

10.12.1 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.

10.12.2 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 o el Boletín Oficial del Estado.

10.12.3 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 10.12.2.

10.13 RECLAMACIONES Y JURISDICCIÓN

Todas reclamaciones entre usuarios y el prestador 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.

10.14 NORMATIVA APLICABLE

Las operaciones y funcionamiento de DNI y de los certificados de firma centralizada, 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:

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- Ley 84/78, 28 de Diciembre que regula la tasa por expedición y renovación del DNI.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- 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.

- Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el 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.
- Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el 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.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.
- Real Decreto 414/2015, de 29 de mayo, por el que se modifica el 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 Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, Título I, Capítulo I, Artículos 3 y 4.
- Real Decreto 557/2011, de 20 de abril por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, Título XIII, Capítulo I, Artículos 205 y 206, Capítulo II, Artículos 207-210 y Capítulo IV, Artículos 213 y 214.
- Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España en ciudadanos de los Estados miembros de la Unión Europea y de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo.
- Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, concretamente ANEXO I Secretaria de Estado de Seguridad, Dirección General de Policía, Ámbito del Cuerpo Nacional de Policía, Punto 3: Adexttra.
- Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones, por las que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

10.15 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.

10.16 ESTIPULACIONES DIVERSAS

10.16.1 Cláusula de aceptación completa

Todos los Terceros Aceptantes asumen en su totalidad el contenido de la última versión de esta DPC.

10.16.2 Independencia

En el caso de que una o más estipulaciones de esta DPC sean o llegasen a ser inválidas, nulas, o inexigibles 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.

10.16.3 Resolución por la vía judicial

No estipulado

10.17 OTRAS ESTIPULACIONES

No se contemplan.

11. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

11.1 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/1202/2011, de 4 de mayo (siendo modificada, entre otros, por Orden INT/1321/2107) por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, en su anexo II, menciona el fichero ADDNIFIL cuya finalidad es la gestión del Documento Nacional de Identidad, sometido al ámbito de aplicación de la Ley vigente en Protección de Datos.

No obstante, se pone a disposición de los prestadores de servicios de validación las listas de certificados revocados para el cumplimiento diligente de los servicios de confianza.

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 así como sometido al ámbito de aplicación de la Ley vigente en Protección de Datos. 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.

De igual forma, Gerencia de Informática de la Seguridad Social (GISS) como encargado de tratamiento de la información únicamente podrá utilizar los datos que le sean facilitados de acuerdo con esas finalidades. Todas las entidades que actúen como prestadores de servicios de confianza deberán a su vez adoptar su correspondiente documento de

seguridad, tal y como exige para el encargado del tratamiento el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

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.

11.2 DOCUMENTO DE SEGURIDAD LOPD

11.2.1 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 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de 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 DNI y de los certificados de firma centralizada, por lo que afecta a todos aquellos recursos (personas, equipos, comunicaciones, software, procedimientos) implicados en el tratamiento de los datos.

11.2.2 Funciones y obligaciones del personal

Esta DPC, así como futuras versiones de la misma, es conocida por todas las personas que acceden a los datos de carácter personal gestionados por DNI y los certificados de firma

centralizada, 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 DNI y de los certificados de firma centralizada.

11.2.3 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:

DATOS TRATADOS
Datos de carácter identificativo
FILIACIÓN
Nombre y apellidos
Fecha y Lugar de Nacimiento
Nombre de los Padres
Sexo
Datos de características personales
Número del DNI
Domicilio
Teléfono
Correo electrónico
Fotografía
Firma
Impresiones dactilares
Número de serie certificado electrónico

En el apartado 8 se recoge la estructura detallada del perfil del certificado.

11.2.4 Nivel de seguridad

Aun 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 DNI y de los certificados de firma centralizada, y el nivel de seguridad que establece esta DPC, se implantarán medidas de seguridad de nivel alto.

11.2.5 Sistemas de información

Dentro de la estructura de sistemas de información que constituye la PKI DNI y de los certificados de firma centralizada 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.
- **Subsistema de publicación:** Se encarga de la gestión de la publicación de las Listas de Revocados (CRL) y del Directorio de certificados.

11.2.6 Relación de usuarios

El Responsable 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 Responsable 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.

11.2.7 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.

11.2.8 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.

11.2.9 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.

11.2.10 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 confianza 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.

11.2.11 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.

11.2.12 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.