INFRAESTRUCTURA DE CLAVE PÚBLICA

DE LA DIRECCIÓN GENERAL DE LA POLICÍA

DECLARACIÓN DE PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN

OID: 2.16.724.1.2.1.102.1.0.5

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

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

1.1 RESUMEN

El presente documento recoge la Declaración de Prácticas y Políticas de Certificación de la DGP que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública encargada de la gestión de los Certificados emitidos para la identificación de la Sede Electrónica de la DGP, para los sistemas de firma electrónica para la actuación administrativa automatizada de dicha Dirección General y para el personal al servicio de la Dirección General de la Policía, almacenados, estos últimos, tanto en el Carné Profesional como en los Documentos de Identidad Profesional, en adelante se referirán ambos documentos por Carné Profesional.

La Dirección General de la Policía emite diferentes tipos de certificados. Inicialmente tres tipos de certificados:

- **Certificados de Empleado Público**, que son emitidos al personal al servicio de la Dirección General de la Policía y tienen el propósito de identificación, firma electrónica reconocida y cifrado de datos, para el desempeño de las funciones propias del puesto que ocupen o para relacionarse con otras Administraciones Públicas cuando éstas lo admitan.
- **Certificados de sello**. Emitidos a organismos o entidades de esta Dirección General con propósito de firma de documentos administrativos en el ámbito de sus funciones.
- **Certificados de sede**. Emitido por y para la Dirección General de la Policía, con el propósito de garantizar la autenticación y cifrado de los canales de comunicación con la Sede Electrónica de la Dirección General de la Policía.

El Real Decreto 1484/1987, de 4 de diciembre, sobre normas generales relativas a escalas, categorías, personal facultativo y técnico, uniformes, distintivos y armamento del Cuerpo Nacional de Policía, promulgado en desarrollo de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, en su Disposición Final segunda faculta al Ministerio del Interior a dictar las disposiciones necesarias para el desarrollo del mismo y, en especial, para determinar el diseño, contenido y características técnicas del Carné Profesional.

En uso de la mencionada habilitación, fue publicada la Orden de 8 de febrero de 1988, por la que se establecen los distintivos, el Carné Profesional, placa emblema y divisas del Cuerpo Nacional de Policía, modificada por la Orden del Ministerio del Interior de 24 de noviembre de 1988, en diversos aspectos referidos al Carné Profesional de los funcionarios del Cuerpo Nacional de Policía.

El tiempo transcurrido desde la publicación de las referidas Órdenes Ministeriales y los avances tecnológicos habidos durante tal periodo, han hecho que el carné aprobado en dichas Ordenes haya quedado obsoleto, por lo que resulto aconsejable acometer la implantación de un **nuevo modelo de Carné Profesional** para los funcionarios del CNP que, acorde con las técnicas más avanzadas, permita un cumplimiento más eficiente de las funciones atribuidas a dicho documento. A estos efectos el nuevo Carné Profesional posibilita tanto la identificación profesional presencial, como la electrónica de sus

titulares, al incorporarse al mismo los dispositivos adecuados que harán posible la firma electrónica avanzada y reconocida en los términos previstos en la **Ley 59/2003**, de **19 de Diciembre**, de firma electrónica.

Por otra parte, la necesidad de impulsar el empleo y la aplicación de técnicas y medios electrónicos, informáticos y telemáticos por la Administración policial, para el desarrollo de la actividad y el ejercicio de las competencias que tiene encomendadas, también hizo aconsejable dotar al resto del personal que presta sus servicios en la Dirección General de la Policía, de un instrumento adecuado a dicho fin como es un **nuevo documento de identidad profesional** que llevará incorporado, al igual que el carné profesional de los funcionarios del Cuerpo Nacional de Policía, la firma electrónica avanzada.

Para ello el Órgano encargado de la expedición y gestión del Carné Profesional – La Dirección General de la Policía, tal y como recoge la Orden INT/761/2007 de 20 de marzo de 2007- implanto una Infraestructura de Clave Pública, que dota al nuevo Carné Profesional y a los otros Documentos de Identidad Profesional, de los certificados electrónicos necesarios para cumplir adecuadamente con los objetivos anteriores

El presente documento recoge la Declaración de Prácticas y Políticas de Certificación (DPC) que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública encargada de la gestión de los Certificados tanto del nuevo Carné Profesional como de los nuevos Documentos de Identidad Profesional, de la Dirección General de Policía. En adelante se referirán ambos documentos por **Carné Profesional**.

Esta DPC no descarta la emisión de otro tipo de certificados (firma de código, timestamping, ocsp responder y otros), cuyas Políticas de Certificación se irán incorporando a este documento a medida que se vayan definiendo.

La DPC se aplica a todos los intervinientes relacionados con la jerarquía de PKI, incluyendo Autoridades de Certificación (AC), Autoridades de Registro, titulares de los certificados y Terceros Aceptantes, entre otros.

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

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

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

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

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.
- 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.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- ORDEN INT/761/2007, de 20 de marzo, por el que se aprueba el nuevo modelo de carné profesional de los funcionarios del Cuerpo Nacional de Policía y otros documentos identificativos.

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

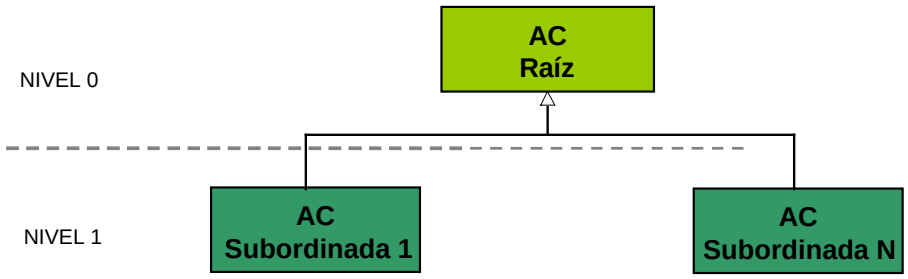
La DPC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía de la relación entre el Carné Profesional y sus usuarios. En consecuencia, todas las partes involucradas tienen la obligación de conocer la DPC y ajustar su actividad a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

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

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

Esta DPC asume que el lector conoce los conceptos de PKI, certificado y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento. El usuario dispondrá en el portal web interno de la Dirección General de la Policía la información necesaria para poder llevar a cabo esta formación.

La arquitectura general, a nivel jerárquico, de la PKI de la Dirección General de la Policía es la siguiente:



- Un primer nivel en el que se ubica la AC raíz que representa el punto de confianza de todo el sistema y que permitirá que todas la personas físicas o jurídicas, públicas o privadas, reconozcan la eficacia de los certificados emitidos por la DGP.
- Un segundo nivel, constituido por las AC subordinadas de la AC Raíz que emitirán los certificados de Sede Electrónica, de Sello Electrónico, de empleado público (identidad, firma y cifrado) del Carné Profesional.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre del documento	Declaración de Practicas y Políticas de Certificación (DPC)
Versión del documento	1.0
Estado del documento	FINAL
Fecha de emisión	24/07/2012
Fecha de caducidad	No aplicable
OID (Object Identifier)	2.16.724.1.2.1.102.1.0.5
Ubicación de la DPC	URL-DPC (En la actualidad http://www.policia.es/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 de Certificados.
- La Autoridad de Aprobación de Políticas.
- Las Autoridades de Certificación.
- Las Autoridades de Registro.
- Las Autoridades de Validación.

- Titulares del Carné Profesional y responsables de otros tipos de certificados emitidos bajo esta DPC.
- Los Terceros Aceptantes de los certificados emitidos por la Dirección General de la Policía, incluyendo Prestadores de Servicios basados en la utilización del Carné Profesional.

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 Publica (PKI), 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 la Orden General de la Dirección General de la Policía.

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 de la Dirección General de la Policía, de determinar la adecuación de la DPC de dicha AC a esta DPC.

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

1.3.2 Autoridades de Certificación

La Dirección General de la Policía actúa como Autoridad de Certificación (AC), a través de la emisión de los correspondientes Certificados de conformidad con los términos de esta DPC.

Las Autoridades de Certificación que componen la PKI de la Dirección General de la Policía son:

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

Nombre Distintivo	CN=AC RAIZ DGP, OU=CNP, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Certificado pkcs1-sha1WithRSAEncryption (*)	
Número de serie	00 bc 2f 63 1d 8e d5 83 7a 53 14 0e 8b 70 71 de
Periodo de validez	Desde jueves, 25 de enero de 2007 13:05:08 hasta domingo, 25 de enero de 2037 13:05:08
Huella Digital (SHA-1)	3B:A2:A1:5F:4D:4A:31:2F:85:66:FE:EA:72:1A:4A:FA:96:DF:D9:7E
Huella Digital (MD5)	25:F9:DA:B6:63:35:55:DA:A5:46:C2:C1:14:B8:B4:9E
Certificado pkcs1-sha256WithRSAEncryption	
Número de serie	00 c2 78 ff aa d1 07 2c 72 a7 8d 2d 24 be 3a 5e
Periodo de validez	Desde jueves, 25 de enero de 2007 13:05:08

	hasta domingo, 25 de enero de 2037 13:05:08
Huella Digital (SHA-1)	60:F3:D3:F9:CC:23:4C:25:9B:27:4E:A7:62:51:69:50:7A:8D:48:91
Huella Digital (MD5)	4A:A7:CC:98:C7:03:39:23:76:E1:B6:D9:B7:A6:E2:1A

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

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

  En el momento de publicación de la presente DPC, el dominio de certificación de la Dirección General de la Policía consta de las siguientes AC subordinadas:

Autoridad de Certificación Subordinada 001

Nombre Distintivo	CN=AC DGP 001, OU=CNP, O=DIRECCION GENERAL DE LA POLICIA, C=ES
Certificado pkcs1-sha1WithRSAEncryption (*)	
Número de serie	19 9d cd 70 a4 dc cf 77 45 d1 84 da 5b d0 3c 04
Periodo de validez	Desde martes, 13 de febrero de 2007 10:09:13 hasta domingo, 13 de febrero de 2022 10:09:13
Estado	Operativa
Huella Digital (SHA-1)	FF:F4:AA:8D:12:E3:C5:E4:D1:2F:4D:1C:80:3B:F3:25:FD:80:6B:BA
Huella Digital (MD5)	92:72:BD:A5:DA:57:89:8D:BD:85:A7:2D:43:6B:36:81
Certificado pkcs1- sha256WithRSAEncryption	
Número de serie	02 70 77 50 e7 ca 7f 3d 45 d1 85 2e b4 aa 0f 40
Periodo de validez	Desde martes, 13 de febrero de 2007 10:09:13 Hasta domingo, 13 de febrero de 2022 10:09:13
Estado	Operativa
Huella Digital (SHA-1)	C6:2C:FF:73:04:90:E5:49:90:94:8A:67:02:62:44:40:A3:53:47:26
Huella Digital (MD5)	39:56:CE:29:24:BF:3D:5D:4E:54:EC:D5:A5:55:B6:3D

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

Autoridad de Certificación Subordinada 002

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

Certificado pkcs1-sha1WithRSAEncryption (*)	
Número de serie	5a 7c c3 d7 16 c3 1f 00 45 cc 60 c2 46 bf 54 4a
Periodo de validez	Desde viernes, 09 de febrero de 2007 12:53:38 Hasta miércoles, 09 de febrero de 2022 12:53:38
Estado	Operativa
Huella Digital (SHA-1)	6B:A4:0A:76:E7:AF:86:A7:B9:5B:94:13:B4:CD:3E:3B:BD:38:A9:7E
Huella Digital (MD5)	F6:F1:08:E6:3F:BD:A9:91:FA:80:51:30:E5:5D:D1:0B
Certificado pkcs1- sha256WithRSAEncryption	
Número de serie	42 39 52 47 75 51 cf 0f 45 cc 61 29 46 14 de 2c
Periodo de validez	Desde viernes, 09 de febrero de 2007 12:55:21 Hasta miércoles, 09 de febrero de 2022 12:55:21
Estado	Operativa
Huella Digital (SHA-1)	6B:25:5E:50:38:66:F5:1C:F2:4A:C3:77:42:2B:E0:03:D6:1F:94:B1
Huella Digital (MD5)	33:49:98:97:13:A5:24:5A:33:08:95:07:30:A3:C0:C4

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

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

1.3.3 Autoridades de Registro

La Autoridad de Registro (AR) es la entidad encargada de garantizar que la solicitud del certificado contiene información veraz y completa y actúa de intermediario entre el usuario final y la Autoridad de Certificación.

La función de autoridad de Registro será realizada:

1. Para los certificados del Carné Profesional:

   El órgano administrativo encargado de la gestión de recursos humanos de la Dirección General de la Policía (en la actualidad la División de Personal de la Subdirección General de Recursos Humanos), será el órgano encargado de la expedición y gestión del Carné Profesional. Dicha expedición tendrá lugar en las oficinas que el mismo tiene en cada una de las dependencias policiales.

   Dado la naturaleza del Carné Profesional, la expedición será realizada por personal propio del Cuerpo Nacional de la Policía.

2. Para los Certificados de la sede electrónica y la actuación administrativa automatizada, así como para cualquier otro tipo de certificados distintos de los asociados al CP (servidor SSL, timestamping y otros):

   La función de registro será realizada por el personal del departamento policial competente (en la actualidad el Área de Informática) de la Dirección General de la Policía.

1.3.4 Autoridad de Validación

La(s) Autoridad(es) de Validación (AV) tienen como función la comprobación del estado de los certificados emitidos por las AC de la DGP, 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."*

Dentro de la infraestructura de Clave Pública de la Dirección General de la Policía se ha desplegado una Autoridad de Validación, tanto para su uso interno por servicios propios de la Dirección General de la Policía, como para su uso externo por prestadores de servicio que confíen en la infraestructura de la DGP. Dicha Autoridad de Validación cumple con los objetivos de universalidad y redundancia.

1.3.5 Titulares del Carné Profesional de la Dirección General de la Policía

El Carné Profesional de los funcionarios del Cuerpo Nacional de Policía, en adelante Carné Profesional, es el documento oficial que acredita la condición de funcionario del referido Cuerpo de sus titulares, que igualmente permitirá a éstos su identificación electrónica, así como la firma electrónica de documentos y el cifrado de datos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Las tarjetas soporte del carné profesional llevan incorporado un chip de contacto donde se almacenan los certificados electrónicos que posibilitan las utilidades indicadas en el párrafo anterior. Las dimensiones de las tarjetas, su diseño, contenido y demás características técnicas son las que se relacionan en el Anexo III de la ORDEN INT/761/2007, de 20 de marzo, por la que se aprueba el nuevo modelo de carné profesional de los funcionarios del Cuerpo Nacional de Policía y otros documentos identificativos.

1.3.6 Titulares de otros documentos identificativos

Con la finalidad de acreditar la identidad profesional y su vinculación con la Dirección General de la Policía, así como la de posibilitar la firma electrónica avanzada y reconocida a sus titulares, la indicada Dirección General expedirá los documentos identificativos correspondientes, al personal que seguidamente se relaciona:

1. Personas que ostenten la titularidad de los Órganos Directivos en el ámbito citado.

2. Alumnos del centro de formación para ingreso y funcionarios en prácticas del Cuerpo Nacional de Policía.
3. Funcionarios de los Cuerpos de la Administración General del Estado o de otras Administraciones Publicas y personal laboral que desempeñen puestos de trabajo en dicha Dirección General.

En lo sucesivo nos referiremos indistintamente al carné profesional y a otros documentos identificativos, bajo el epígrafe de carné profesional, siendo análogos dichos documentos a los efectos de esta DPC.

1.3.7 Terceros aceptantes

Los Terceros Aceptantes son las personas o entidades ajenas a la Dirección General de la Policía que deciden aceptar y confiar en un certificado emitido por la misma.

Se entiende como prestador de servicios a toda persona física o jurídica que ofrece la posibilidad de realizar transacciones telemáticas utilizando el Carné Profesional.

1.4 USO DE LOS CERTIFICADOS

1.4.1 Usos apropiados de los certificados

Los certificados emitidos por la Dirección General de la Policía serán utilizados para dar cumplimiento a las funciones que le son propias y legítimas, y para el desempeño de las funciones propias del personal al servicio de dicha Dirección General. Se emitirán de acuerdo con lo establecido en el artículo 11 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y se cumplirán las obligaciones determinadas en dicha Ley y en las normativas específicas vigentes en el ámbito de la Administración General del Estado.

1. **Los Certificados de sede**, emitidos por la Dirección General de la Policía se utilizaran para la identificación de la sede electrónica y para el establecimiento de comunicaciones seguras con ellas.
2. **Los Certificados de sello** emitidos por la Dirección General de la Policía se utilizarán para garantizar la identificación y autenticación del ejercicio de las competencias del órgano o entidad titular en la actuación administrativa automatizada.
3. **Los Certificados del Carné Profesional**, emitidos por la Dirección General de la Policía, se utilizaran para el desempeño de las funciones propias del personal al servicio de dicha Dirección General, tendrán como finalidad:
   - **Certificado de Autenticación:** Garantizar electrónicamente la identidad del funcionario 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 Carné Profesional 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 reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

Este certificado lleva asociada a la identidad (nombre, apellidos y DNI/NIE) la capacidad profesional del titular, con la incorporación al certificado de la siguiente información adicional:

- Categoría profesional
- Dirección de correo corporativo
- Número de Carné profesional
- Identificador único del titular en los Sistemas de Información de la Dirección General de la Policía

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

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

  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).

  Este certificado lleva asociada a la identidad (nombre, apellidos y DNI/NIE) la siguiente información adicional:

  - Categoría profesional
  - Número de Carné profesional

- **Certificado de Cifrado**: Permitir el intercambio de información de manera segura, de tal manera que sólo el titular del certificado sea capaz de acceder a dicha información.

  Los certificados de cifrado pueden utilizarse para prestar los siguientes servicios de seguridad:

  - Cifrado de correos electrónicos
  - Cifrado de ficheros
  - Cifrado de transacciones

  El uso del certificado de cifrado se limitará a ámbito profesional, quedando expresamente prohibido el uso personal del mismo; el titular del certificado debe ser consciente que la Dirección General de la Policía, almacena el material criptográfico asociado con el certificado de cifrado para su recuperación en caso de emergencia.

  Este certificado lleva asociada a la identidad (nombre, apellidos y DNI/NIE) la siguiente información adicional:

  - Categoría profesional
  - Dirección de correo profesional
  - Número de Carné profesional

El uso conjunto de los certificados anteriores proporciona las siguientes garantías:

- Autenticidad de origen

  El Funcionario 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 Carné Profesional, el cual dispone de un procesador con capacidades criptográficas. Esto permite garantizar que la clave privada del titular (punto en el que se basa la credibilidad de su identidad) no abandona en ningún momento el soporte físico del Carné Profesional. De este modo el titular, en el momento de acreditar electrónicamente su identidad, deberá estar en posesión de su Carné Profesional y de la clave personal de acceso (PIN) a la clave privada del certificado.

- No repudio de origen

  Asegura que el documento proviene del titular 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 el servicio de validación ofrecido por la Dirección General de la Policía. De esta forma se garantiza que el documento proviene de un determinado funcionario.

  Dado que el Carné Profesional es un dispositivo de creación de firma y que las claves de firma permanecen desde el momento de su creación bajo el control del 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.

- Confidencialidad

  Mediante el uso del **Certificado de Cifrado** se garantiza que únicamente el destinatario del mensaje es capaz de acceder al contenido del mismo.

  El emisor del mensaje, haciendo uso del certificado de cifrado del receptor, es capaz de cifrar la información contenida en dicho mensaje, de tal manera que sólo el receptor, en posesión de clave privada asociada al certificado, o personal autorizado actuando de oficio, sean capaces de acceder al contenido del mismo. Los procedimientos de archivo y recuperación de claves se describen en detalle en el apartado “4.12 Custodia y recuperación de claves”

  El servicio encargado de la custodia y acceso a los certificados de cifrado y su clave privada asociada se denomina *Servicio de Archivo y Recuperación de Claves*. La descripción se este servicio se encontrará más adelante en este mismo documento.

1.4.2 Limitaciones y restricciones en el uso de los certificados

Los certificados emitidos por la Dirección General de la Policía 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 no pueden utilizarse para actuar ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

Los certificados de Sede y de Sello no se utilizaran para fines distintos de los especificados en la presente Declaración de Practicas de Certificación.

Los certificados del Carné Profesional podrán emplearse para autenticación (acreditación de identidad), firma electrónica (no repudio y compromiso con lo firmado) y confidencialidad (cifrado).

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 certificación que ofrece la Dirección General de la Policía, 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 Carné Profesional es un dispositivo de creación de firma y como tal, garantiza que las claves de firma y autenticación permanecen desde el momento de su creación bajo el control del titular y no es posible su exportación y uso desde cualquier otro dispositivo.

Respecto a la clave de cifrado, esta es generada externamente a la tarjeta, importada en la misma y custodiada adicionalmente por el Servicio de Archivo y Recuperación de Claves, de tal manera que pueda ser recuperada en el caso de que el titular, o persona autorizada, lo requiera.

El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de su carné profesional así como de los mecanismos de activación de las claves privadas, evitando su pérdida, divulgación, modificación o uso no autorizado.

1.5 ADMINISTRACIÓN DE LAS POLÍTICAS

1.5.1 La Dirección General de la Policía como Órgano responsable de la Infraestructura de Clave Pública.

Esta DPC es propiedad de la Dirección General de la Policía:

Nombre	Dirección General de la Policía		
Dirección e-mail	carnetprofesional@policia.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) de la Infraestructura de Clave Pública de la Dirección General de la Policía.

Nombre	Grupo de trabajo de la Infraestructura de Clave Pública de la Dirección General de la Policía		
Dirección e-mail	carnetprofesional@policia.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 la Infraestructura de Clave Pública de la DGP.

En el caso de que se tuviese que evaluar la posibilidad de que una AC externa interactúe con la PKI de la Dirección General de la Policía estableciendo relaciones de confianza, la Autoridad de Aprobación de Políticas (AAP) 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 la Infraestructura de Clave Pública de la Dirección General de la Policía 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:

Actuación administrativa automatizada: Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

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 Carné Profesional el dato de activación es la clave personal de acceso (PIN) y/o el código de desbloqueo del PIN (PUK)

Autenticación: procedimiento de comprobación de la identidad de un solicitante o titular de certificados del Carné Profesional

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

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

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

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

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

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

Código de Desbloqueo (PUK): Secuencia de caracteres que permiten el desbloqueo del PIN para su reseteo en el Carné Profesional.

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

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

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

Dispositivo de creación de Firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

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

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

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

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

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

Firma electrónica avanzada: es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor,

como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

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

Funcionario (en el contexto de esta DPC): A todo el personal funcionario perteneciente al Cuerpo Nacional de la Policía, se le asignará la expedición o renovación de un Carné Profesional, por un funcionario del mismo cuerpo asignado a tal efecto. Únicamente podrán ser titulares del Carné Profesional los funcionarios de la Dirección General de la Policía durante su permanencia en las situaciones administrativas de activo y de segunda actividad.

Así mismo, todo el personal que presta sus servicios en la Dirección General de la Policía, se le proporcionará un documento identificativo profesional que lo requiera para el desempeño de sus funciones.

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 del Carné Profesional

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 la Infraestructura de Clave Pública de la Dirección General de la Policía, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.

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

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

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

Solicitante: persona que solicita un certificado para sí mismo

Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por la Dirección General de la Policía.

Titular: Funcionario o personal que presta sus servicios en la Dirección General de la Policía, para el que se expiden los certificados del Carné Profesional

1.6.2 Acrónimos

AAP: Autoridad de Aprobación de Políticas

AC: Autoridad de Certificación

AR: Autoridad de Registro

AV: Autoridad de Validación.

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

CEN: Comité Européen de Normalisation (Comité Européo de Normalización)

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

CNP: Cuerpo Nacional de la Policía.

CP: Carné Profesional de los funcionarios del Cuerpo Nacional de la Policía y otros documentos identificativos para determinado personal que presta sus servicios en la Dirección General de la Policía.

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

FCR: Parámetro asociado a las Funciones Criptográficas de Resumen que en la actualidad es: SHA-1/SHA-256

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

GN: Given Name (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.

ISO: International Organization for Standardization

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 Identificación 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.

PC: Política de certificación

PIN: Personal Identification Number

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.

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

RSA: Rivest-Shimar-Adleman

SA: Parámetro del Algoritmo de Firma utilizado que en la actualidad tiene los valores sha256withRsaEncryption1/sha1withRsaEncryption

SHA: Secure Hash Algorithm

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

TC-AC-R: Tamaño en bits de las claves de la AC Raíz (en la actualidad es de 4096 bits).

TC-AC-S: Tamaño en bits de las claves de las AC Subordinadas (en la actualidad es de 2048 bits).

TC-C-SS: Tamaño en bits de las claves de los certificados de Sede electrónica y de Sello (en la actualidad será como mínimo de 2048 bits).

TC-C-CP: Tamaño en bits de las claves de los certificados del Carné Profesional (en la actualidad es de 2048 bits).

TV-C-CP: Tiempo de vigencia máxima en meses de los certificados electrónicos reconocidos incorporados al Carné Profesional (36 meses en la actualidad)

TSL: Transport Layer Security

URL-AC-R: URL de los certificados de la AC RAIZ (en la actualidad: http://www.policia.es/certs/ACraiz.crt)

URL-AC-S: URL de los certificados de las AC Subdordinadas (en la actualidad: http://www.policia.es/certs/ACXXX.crt)[2]

URL-ARL: URL de la lista de AC revocadas (en la actualidad: http://crls.policia.es/crls/ARL.crl)

URL-DPC: URL de publicación de la DPC (en la actualidad http://www.policia.es/dpc)

URL-OCSP: URL del Servicio de validación en línea del estado de los certificados OCSP (en la actualidad http://ocsp.policia.es)

---

[1] Se utilizara *sha1withRsaEncryption* para la garantizar la compatibilidad con las aplicaciones y sistemas que actualmente no soportan *sha256withRsaEncryption*.

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

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

El servicio de repositorio de certificados está disponible durante las 24 horas de los 7 días de la semana.
Toda la información publicada estará disponible en la página Web de la Dirección General de la Policía (www.policia.es)

Para los certificados de la AC Raíz y ACs Subordinadas:

- URL-AC-R (en la actualidad: http://www.policia.es/certs/ACraiz.crt)
- URL-AC-S (en la actualidad: http://www.policia.es/certs/ACXXX.crt)[3]

Para la lista de AC revocadas (ARL):

- URL-ARL (en la actualidad: http://crls.policia.es/crls/ARL.crl)

Para la DPC:

- URL-DPC (en la actualidad http://www.policia.es/dpc)

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

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

Servicio de validación en línea que implementa el protocolo OCSP:

- URL-OCSP (en la actualidad: http://ocsp.policia.es)

El repositorio de la PKI de la Dirección General de la Policía 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 las direcciones de Internet https://sede.policia.gob.es y http://www.policia.es/ y a través de la Orden General de la Dirección General de la Policía.

Será responsabilidad de la Dirección General de la Policía la adopción de las medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

Tanto los funcionarios 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

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

Policía, accediendo a las direcciones de internet https://sede.policia.gob.es y a la correspondiente a URL-DPC donde se encontrará firmada electrónicamente.

Las Listas de Certificados Revocados estarán firmadas electrónicamente y estarán disponibles tanto para los servicios internos de la Dirección General de la Policía, como para aquellos prestadores de servicios que confíen en la infraestructura de clave Pública de la Dirección General de la Policía.

La información sobre el estado de los certificados se podrá consultar mediante el servicio de validación en línea que implementa el protocolo OCSP. Este servicio está disponible desde la intranet de la policía, para los servicios internos de la Dirección General de la Policía, como desde Internet para aquellos prestadores de servicios que requieran la validación de certificados emitidos por la infraestructura de la DGP.

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 de la Infraestructura de Clave Pública de la Dirección General de la Policía se llevará a cabo en las direcciones de Internet de la Dirección General de la Policía (https://sede.policia.gob.es y http://www.policia.es) y a través de la Orden General de dicha Dirección General.

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 la misma. Cuando se realicen modificaciones significativas en la DPC de la Infraestructura de Clave Pública de la Dirección General de la Policía, éstas se notificarán en la dirección de Internet de la Dirección General de la Policía (https://sede.policia.gob.es y http://www.policia.es) y a través de la Orden General de dicha Dirección General.

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

Servicio de validación en línea

El servicio de validación mantendrá, en todo momento, la información actualizada del estado de los certificados emitidos por las Autoridades de Certificación de la Infraestructura de Clave Pública de la Dirección General de la Policía.

En caso de producirse una modificación en el estado de un certificado, el servicio de validación conocerá este hecho inmediatamente.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso para la lectura a los repositorios anteriores (certificados de AC, ARLs, DPC y Políticas) es abierto, pero sólo la AAP de la Infraestructura de Clave Pública de la

Dirección General de la Policía está autorizada a modificar, sustituir o eliminar información de su repositorio y sitio web. Para ello la Dirección General de la Policía establecerá controles que impidan a personas no autorizadas manipular la información contenida en los repositorios.

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

3.1 NOMBRES

En esta sección se establecen los procedimientos de identificación y autenticación que se utilizan durante el registro de los suscriptores, que se realizaran con anterioridad a la emisión y entrega de certificados.

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.500 en el campo Subject, incluyendo un atributo Common Name (CN).

Se incluye en estos certificados la siguiente información:

• Country: ES (corresponde al código ISO de país, correspondiente al Estado Español).

• Organizational Unit Name: El nombre del tipo de servicio de certificación que se presta.

• Surname: Los apellidos del suscriptor, autorizado por la Entidad de Registro

• Given Name: El nombre del suscriptor, autorizado por la Entidad de Registro

• Serial Number: DNI/NIE., del suscriptor, autorizado por la Entidad de Registro

• Common Name: El nombre en texto libre del suscriptor, autorizado por la Entidad de Registro

Los certificados emitidos para el Carné Profesional 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 DGP XXX

OU=CNP

O=DIRECCIÓN GENERAL DE LA POLICÍA

C=ES

Donde XXX es un identificador de tres dígitos

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

CN= <NOMBRE> <APELLIDO1> <APELLIDO2> - [DNI][NIE] <Número del DNI/NIE> [AUTENTICACIÓN][FIRMA][CIFRADO]

GN=<NOMBRE>

SN=<APELLIDO1> <APELLIDO2> - [DNI][NIE] <Número del DNI/NIE>

NÚMERO DE SERIE=<DNI/NIE> (Número personal del Documento Nacional de Identidad, o del Numero de Identificación de Extranjero, y carácter de verificación correspondiente)

OU = AMBITO DEL CUERPO NACIONAL DE POLICIA

OU = EMPLEADO PUBLICO

O = MINISTERIO DE INTERIOR

C = ES

En el atributo CN (Common Name) del certificado se facilita al usuario la identificación del tipo de certificado, incluyendo al final de dicho atributo la finalidad para la que se expidió el certificado.

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 Carné Profesional 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 del CP, 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, siendo únicos, para cada servicio de generación de certificados operado por la Dirección General de la Policía.

En los certificados del CP la utilización del número del DNI/NIE del funcionario garantiza la unicidad del DN.

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

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

La pertenencia de los diferentes organismos o entidades solicitantes de los certificados de Sede o Sello a la Dirección General de la Policía, garantiza la capacidad de ésta de autenticar y acreditar la identidad de los suscriptores.

La clave privada se genera en el interior del servidor en el que se instalará los certificados de sede electrónica o sello, quedando probada la posesión de la misma por el envío de la correspondiente clave pública al departamento policial competente (en la actualidad el Área de Informatica) mediante un paquete PKCS#10. En aquellos casos en que no sea posible su generación interna, la clave privada será generada por el departamento policial competente (en la actualidad el Área de Informatica) y se le enviará al solicitante mediante un correo electrónico cifrado y con acuse de recibo.

Los dos pares de claves asociados a los certificados del Carné Profesional, de autenticación y firma se generan en presencia del funcionario utilizando un dispositivo de creación de firma (la tarjeta criptográfica soporte del Carné Profesional), 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 Carné Profesional. Las claves privadas, de autenticación y firma, 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 del Carné Profesional.

La clave de cifrado es generada en el momento de expedición del Carné Profesional, en un dispositivo criptográfico (HSM) externo e inyectada en la tarjeta con el mismo nivel de seguridad y condiciones de acceso que los otros dos pares de claves. La clave pública, de cifrado será enviada junto a las otras claves públicas de autenticación y firma, a la AC para que esta genere los certificados correspondientes. Así mismo todo el material criptográfico de cifrado, se almacenará en un repositorio externo de claves de cifrado para permitir su recuperación por parte del titular o persona autorizada.

3.2.2 Autenticación de la identidad de una persona jurídica

No estipulado.

3.2.3 Autenticación de la identidad de una persona física

La identificación y autenticación del titular del CP para la solicitud de los certificados de identidad, firma electrónica y cifrado seguirá un proceso integrado con el registro para la expedición del Carné Profesional.

Por lo tanto, el funcionario cuando recoja, por primera vez, su Carné Profesional, deberá comparecer el departamento de personal de su plantilla de destino, presentando su Documento Nacional de Identidad al funcionario encargado de la expedición y gestión del Carné Profesional.

El Carné Profesional se entregará a los titulares personalmente junto con las claves personales secretas (PIN y PUK) que les haya sido asignada. Dichas claves personales secretas se imprimirán en papel en el momento de la generación de los certificados y se entregará al funcionario junto con su Carné Profesional.

Si el titular del Carné Profesional varía la categoría, o la situación administrativa, que tenía al momento de la expedición, se le hará entrega de un nuevo Carné Profesional, acorde con la nueva categoría o situación administrativa, a la que el mismo hubiese accedido. Esta **renovación** se llevará a cabo mediante la presencia física del titular en el departamento de personal de su plantilla de destino. También se deberá proceder a la renovación del Carné Profesional en el caso de que este no pueda servir adecuadamente a su función identificadora.

El **extravío, sustracción, destrucción o deterioro** del Carné Profesional, 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.

Todos los casos anteriores tienen consigo la pérdida de validez del Carné Profesional, que además llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. Tanto la renovación del Carné Profesional o la expedición de duplicados del mismo implicará, a su vez, la revocación de los certificados vigentes y la expedición de nuevos certificados electrónicos.

A la extinción de la vigencia de los certificados electrónicos (o treinta días antes de dicha extinción), sin que medie la extinción de la vigencia del soporte (tarjeta), podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Carné Profesional. Para la solicitud de un nuevo certificado también deberá mediar **la presencia física** del titular en el departamento de personal de su plantilla de destino y solicitar la renovación

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 el departamento de personal de su plantilla de destino

3.2.4 Información no verificada sobre el solicitante

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

3.2.5 Comprobación de las facultades de representación

No estipulado

3.2.6 Criterios para operar con AC externas

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

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

3.3.1 Identificación y autenticación por una renovación de claves de rutina

La renovación rutinaria de los certificados de Sede o Sello de la Dirección General de la Policía seguirá los mismos pasos establecidos para la validación inicial de la identidad.

En el caso de los certificados del CP se distinguen dos casos:

- Renovación de claves sin renovación del soporte físico (tarjeta): la identificación y autenticación se hará mediante los certificados del Carné profesional, aun no estando estos en vigor. La renovación se deberá efectuar en un puesto de expedición atendido por un funcionario, situado en las Oficinas de Expedición del Carné Profesional. Es de aplicación lo establecido en el apartado 3.2.3
- Renovación de claves por sustitución del soporte físico (tarjeta): Se hará de igual forma que cuando se entrega por primera vez el Carné Profesional, siendo necesaria la presencia física del titular, tal como recoge el apartado 3.2.3.

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

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

Para todos los casos será de aplicación lo contemplado en el punto anterior.

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 Sede electrónica, de Sello y del Carné Profesional (autenticación, firma electrónica y cifrado).

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 Quién puede efectuar una solicitud

La emisión de los certificados de Sede Electrónica o de Sello se realiza a petición de los órganos o entidades pertenecientes a la Dirección General de la Policía. La solicitud la realizará la persona física habilitada para ello en cada órgano o entidad de que se trate.

Los certificados del CP se otorgarán de oficio para el personal que presta sus servicios en la Dirección General de la Policía. El ciclo de vida de estos certificados está totalmente integrado con el de la tarjeta soporte del Carné Profesional. La emisión del documento y de los certificados asociados se realizará en una sola visita al departamento de personal de su plantilla de destino del personal al servicio de esta Dirección General.

4.1.2 Registro de las solicitudes de certificados

El departamento policial competente (en la actualidad el Área de Informatica) asegura que las solicitudes de certificados son completas, precisas y están debidamente autorizadas.

Para los certificados de Sede electrónica y de Sello la solicitud se realiza mediante un formulario en el que deberán constar los datos del órgano o entidad titular del certificado de Sede, o del de Sello, y los de la persona física autorizada que lleva a cabo dicha solicitud. La solicitud será firmada de forma manuscrita, o electrónicamente, por este representante y remitida al departamento policial competente (en la actualidad el Área de Informatica). Dicho departamento policial será el encargado de comprobar que todos los datos son correctos antes de proceder a la emisión del certificado.

En el caso del CP la obtención de los certificados de autenticación, firma electrónica y cifrado está ligada a la obtención de la tarjeta soporte del Carne Profesional.

El órgano administrativo encargado de la gestión de recursos humanos de la Dirección General de la Policía (en la actualidad La División de Personal de la Subdirección General de Recursos Humanos) dará la orden de expedición de un Carné Profesional, ya sea debido a la primera emisión del carné, o por renovación. Esta orden implica la impresión física de la tarjeta soporte del Carné Profesional con los datos relativos al titular del mismo, incluida la fotografía.

Los funcionarios deberán aportar una fotografía reciente en color de su rostro, de uniforme o con chaqueta y corbata oscuras de un solo color sin dibujos sobre camisa blanca, y de tamaño 32 por 26 milímetros, tomada de frente y con la cabeza descubierta.

Para el personal que presta sus servicios en la Dirección General de la Policía deberán aportar una fotografía reciente en color de su rostro, tamaño 32 por 26 milímetros,

tomada de frente y con la cabeza descubierta, que en los supuestos de titulares de Órganos directivos miembros del Cuerpo Nacional de Policía y de los alumnos y funcionarios en prácticas deberá ser también de uniforme.

Una vez impresa la tarjeta, esta será enviada al departamento de personal de la plantilla de destino a la que corresponde el funcionario, el cual deberá acudir a dicha oficina para recoger su tarjeta y, por tanto, los certificados asociados. Los equipos de expedición corresponderán a los equipos que el órgano administrativo encargado de la gestión de recursos humanos de la Dirección General de la Policía (en la actualidad la División de Personal de la Subdirección General de Recursos Humanos) tiene en las distintas dependencias policiales.

Para obtener el Carné Profesional será imprescindible la presencia física de la persona a quién se haya de expedir, junto con su Documento Nacional de Identidad Tarjeta de Identidad de Extranjero, en el caso de la primera emisión del carné profesional o renovación por sustracción, extravío, destrucción o deterioro, o con su Carné Profesional en el caso de renovación del mismo.

La fase de personalización lógica comenzará con la carga de datos en el chip de la tarjeta soporte y con la generación de los pares de claves asociados a los certificados de autenticación y firma electrónica.

La generación de claves de identificación y firma electrónica se realizará en la tarjeta y en presencia del titular, tras la habilitación de una clave personal de acceso –PIN- que se entregará al funcionario. El PIN se habilitará inicialmente con el número del DNI/NIE y la letra de este, correspondiente al titular del CP y podrá ser modificada con la herramienta que para éste propósito proporciona el Area de Informática. Dicho PIN 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. Se recomienda por tanto cambiar la clave personal de acceso – PIN –por otra de la elección del titular del CP.

La clave de cifrado también es generada en el momento de expedición del Carné Profesional, en un dispositivo criptográfico (HSM) externo e inyectada en la tarjeta con el mismo nivel de seguridad y condiciones de acceso que los otros dos pares de claves. La clave pública, de cifrado será enviada junto a las otras claves públicas de autenticación y firma, a la AC para que esta genere los certificados correspondientes. Así mismo todo el material criptográfico de cifrado, se almacenará en un repositorio externo de claves de cifrado para permitir su recuperación por parte del titular o persona autorizada

El proceso de personalización, también genera una clave de desbloqueo (PUK) que se entrega al titular de la tarjeta junto con el PIN. El PUK no puede ser modificado por el usuario. Una copia del mismo es custodiada por el sistema de archivo y recuperación de claves, para permitir su recuperación por parte del titular en caso de pérdida. El PUK permite el desbloqueo de la tarjeta en caso de olvido del PIN o bloqueo de la tarjeta al haber superado el número máximo de intentos de acceso con un PIN incorrecto.

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

4.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 Realización de las funciones de identificación y autenticación

Para los certificados de Sede electrónica y Sello, el departamento policial competente (en la actualidad el Área de Informatica), como Entidad de Registro, procederá a la emisión del certificado correspondiente una vez comprobada la identidad del solicitante y verificada la documentación recibida.

Para los Certificados del CP las funciones de identificación y autenticación descritas en el punto 3.2.3 las realizaran los funcionarios y el personal encargado de la operación de los Equipos de Expedición del Carné Profesional.

Los funcionarios asignados a tal efecto para la expedición del Carné Profesional, desempeñarán el rol de operador de registro, haciendo uso de su propio Carné Profesional, como dispositivo de creación de firma para el control de acceso a la aplicación de expedición y control de integridad y no repudio de las operaciones y transacciones realizadas.

4.2.2 Aprobación o denegación de las solicitudes de certificados

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 certificados, haciendo uso de su propio Carné Profesional
- En el caso del CP, se verificara que la petición procede de una tarjeta de Carné Profesional válida (todas las tarjetas soporte de Carné Profesional dispondrán de un par de claves y un certificado de componente vinculado al número de serie del chip).
- Consta de toda la información necesaria para habilitar los campos y extensiones del certificado de acuerdo con los perfiles definidos.

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

4.2.3 Plazo para la tramitación de las solicitudes de certificados

No estipulado.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 Actuaciones de la AC durante la emisión de los certificados

Después de la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone el certificado a disposición del suscriptor.
Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados, ya que ésta implica la emisión de un nuevo certificado y la generación de nuevas claves.

Para los certificados de Sede y Sello, la emisión del certificado, y en su caso la generación de las claves, tendrán lugar una vez que el departamento policial competente (en la actualidad el Área de Informática) haya introducido los datos en la aplicación de registro. La AC firmará los certificados, y en su caso las claves, y los enviará al solicitante por correo electrónico cifrado y con acuse de recibo.

Los certificados del CP se pondrán a disposición del suscriptor insertándolos en la tarjeta soporte del Carné Profesional, como etapa final en el proceso de personalización lógica de la misma.

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 funcionario insertándolos en la tarjeta soporte del Carné Profesional, como etapa final en el proceso de personalización lógica de la misma.

Los tres certificados, autenticación, firma y cifrado, 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 de la Dirección General de la Policía emita un certificado de acuerdo con una solicitud de certificación efectuará las notificaciones que se establecen en el apartado 4.3.2 del presente capítulo.

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

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

La emisión de los certificados de Sede y Sello se notificara al solicitante por correo electrónico cifrado y con acuse de recibo.

El solicitante de los certificados del Carné Profesional conocerá su emisión efectiva con la entrega de la tarjeta soporte del Carné Profesional.

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

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 Forma en la que se acepta el certificado

Los certificados de Sede electrónica y Sello se considerarán aceptados una vez que quede constancia de la recepción de los mismos por el suscriptor, sin que exista comunicación en contra de rechazo o solicitud de modificación de los datos contenidos en el mismo en un plazo de 10 días hábiles.

Todo funcionario que reciba su Carné Profesional estará obligado a la aceptación de los certificados debido a que, en cualquier momento, las obligaciones de su cargo pueden requerir el uso de los mismos.

Por lo tanto, el funcionario no podrá solicitar la revocación de los certificados emitidos como parte del proceso de expedición, y la aceptación del Carné Profesional conllevará la aceptación explícita de los certificados, independientemente que se hayan obtenido tras la primera inscripción o en las renovaciones posteriores.

4.4.2 Publicación del certificado por la AC

Solo se publicaran los certificados de cifrado del CP que se almacenarán en el directorio LDAP de los Sistemas de Información de la Dirección General de la Policía para facilitar la recuperación del certificado asociado al destinatario de un mensaje o documento cifrado. Asimismo se almacenarán, junto con el par de claves asociado, en el repositorio o archivo de claves de la PKI de la Dirección General de la Policía.

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

La utilización de los certificados de Sede y de Sello atenderá a los usos previstos en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y en su normativa de desarrollo.

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

Los Certificados asociados al Carne Profesional, emitidos por la Dirección General de la Policía tendrán como finalidad:

Certificado de Autenticación: garantizar electrónicamente la identidad del funcionario.

Certificado de Firma: permitir la firma electrónica avanzada de documentos.

Certificado de cifrado: permitir el cifrado/descifrado de información dirigida al titular del carné profesional.

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

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

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

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

4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

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

4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

4.7.1 Circunstancias para una renovación con cambio claves de un certificado

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

La renovación de certificados de Sede electrónica y Sello seguirá el mismo procedimiento que el especificado para la emisión inicial de los mismos, mediante el envío del formulario correspondiente.

La validez del Carné profesional y de sus certificados electrónicos está reflejada por los siguientes puntos:

1. El carné profesional tendrá validez mientras sus titulares ostenten la misma categoría y situación administrativa que tenían al momento de la expedición, debiendo procederse por la Administración a la retirada de los mismos cuando varíe alguna de ellas.
2. En el supuesto de cambio de categoría del titular, en el mismo momento en que tenga lugar la retirada, se le hará entrega al funcionario de un nuevo carné profesional, acorde con la categoría a que el mismo hubiese accedido. En el caso de cambio de situación administrativa, únicamente se le hará entrega de otro Carné Profesional, con sus correspondientes certificados, si la nueva situación administrativa fuera la de Segunda Actividad.
3. Asimismo, con el fin de que los carnés profesionales puedan servir adecuadamente a su función identificadora, la Dirección General de la Policía podrá, bien de oficio en el momento que se considere necesario, o a instancia de los titulares, proceder a la renovación de aquellos carnés que, por el tiempo trascurrido desde su expedición, hayan podido perder las funcionalidades de identificación de sus titulares o se hallen deteriorados.
4. Los certificados electrónicos reconocidos incorporados al Carné Profesional tendrán una vigencia máxima de TV-C-CP meses (36 meses en la actualidad) desde la fecha de su expedición, debiendo procederse de oficio por la Dirección General de la Policía, al finalizar la misma, a la expedición de nuevos certificados.

   La caducidad de los certificados será notificada a su titular mediante un mensaje de aviso proporcionado por la herramienta de acceso al Carné Profesional.
5. También serán causas de extinción de la vigencia de los certificados electrónicos aludidos anteriormente, las establecidas en la Ley 59/2003, de 19 de diciembre, de firma electrónica, que resulten de aplicación. En estos casos, el titular o, en caso de fallecimiento, sus familiares deberán comunicar a la Dirección General de la Policía tal circunstancia, al objeto de que se proceda a la retirada del carné y revocación de los certificados.

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 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 Carné Profesional
- Renovación por caducidad de los certificados sin que medie un cambio de soporte. Esta solicitud podrá realizarse desde los puestos de expedición, ante un funcionario asignado a la expedición del Carné Profesional de las oficinas de expedición del departamento de personal de su plantilla de destino, en un periodo de tiempo que comienza treinta días antes de la fecha de caducidad.

  La notificación de que los certificados están próximos a expirar será realizada por las herramientas de acceso al Carné Profesional.

4.7.2 Quién puede pedir la renovación de un certificado

Para los certificados de Sede electrónico y de Sello, la solicitud únicamente la podrá realizar la persona física habilitada para ello en cada órgano o entidad de que se trate.

El órgano administrativo encargado de la gestión de recursos humanos de la Dirección General de la Policía (en la actualidad la División de Personal) será la encargada, en los supuestos de variación de datos, de proceder a la renovación del Carné Profesional, notificando de tal circunstancia al funcionario titular, para que este recoja su nuevo carné y se proceda a la renovación de los certificados y las claves (renovación con cambio de claves).

El extravío, sustracción, destrucción o deterioro del Carné Profesional, conllevará la obligación de su titular de poner en conocimiento de su superior jerárquico tal circunstancia y de solicitar la expedición de un duplicado del mismo, sin perjuicio de la instrucción del oportuno expediente de averiguación de causas a fin de determinar si el funcionario incurrió en alguna conducta de las tipificadas y sancionadas en el vigente reglamento de régimen disciplinario de los funcionarios del Cuerpo Nacional de Policía

La expedición de duplicados del Carné Profesional, por alguna de las causas relacionadas en el párrafo anterior, supondrá la anulación del anterior, así como la de los certificados electrónicos reconocidos incorporados al mismo.

4.7.3 Tramitación de las peticiones de renovación con cambio de claves

La renovación de certificados de Sede electrónica y Sello seguirá el mismo procedimiento que el especificado para la emisión inicial de los mismos, mediante el envío del formulario correspondiente.

En los certificados del CP se dan los siguientes escenarios:

- Cuando medie la renovación del soporte físico por variación de datos.

  Dicha renovación se llevará a cabo mediante la presencia física del titular del Carné Profesional.

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

Al entregar el Carné Profesional renovado, se procederá a la retirada del anterior para su inutilización física.

Todo el proceso deberá ser realizado en un puesto de expedición atendido por un funcionario, el cual deberá estar autorizado para la expedición del Carné Profesional y pertenecer al departamento de personal de la plantilla de destino del titular del Carné Profesional.

- En los casos de extravío, sustracción, destrucción o deterioro del Carné Profesional

  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.

  En los casos que se disponga de Carné Profesional, se procederá a su retirada para su inutilización física. 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, el cual deberá estar autorizado para la expedición del Carné Profesional y pertenecer al departamento de personal de la plantilla de destino del titular del Carné Profesional.

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

  Desde treinta días antes de la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Carné Profesional. La tramitación se llevará a cabo desde los puestos de expedición del órgano administrativo encargado de la gestión de recursos humanos de la Dirección General de la Policia (en la actualidad la División de Personal de la Subdirección General de Recursos Humanos), frente a un funcionario autorizado para la expedición del Carné Profesional, encargado de validar la identidad del solicitante. Los certificados tendrán como fecha de entrada en vigor el instante en que haya sido generado y como periodo de validez TV-C-CP meses (36 meses en la actualidad). Los certificados vigentes hasta el momento serán eliminados de la tarjeta tras solicitar su revocación.

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

Se utilizara el procedimiento descrito en el apartado 4.3.2 Notificación al solicitante de la emisión por la AC del certificado.

4.7.5 Forma de aceptación del certificado con nuevas claves

Se consideran las mismas condiciones que para el caso de la emisión inicial de certificados, señaladas en el apartado 4.4.1 Forma en la que se acepta el certificado.

4.7.6 Publicación del certificado con las nuevas claves por la AC

Solo se publicaran los certificados de cifrado del CP que se almacenarán en el directorio LDAP de los Sistemas de Información de la Dirección General de la Policía.

Asimismo se almacenarán, junto con el par de claves asociado, en el repositorio o archivo de claves de la PKI de la Dirección General de la Policía.

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

No se permitirá la modificación de los certificados emitidos.
Cualquier circunstancia que obligue a efectuar modificaciones en los certificados emitidos se tratará como una renovación de los mismos, siendo de aplicación los apartados anteriores.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación y suspensión de los certificados 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. En consecuencia, la revocación de un certificado inhabilita el uso legítimo del mismo por parte del titular.

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 del servicio de validación propio de la Dirección General de la Policía.

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

No se contempla la revocación individual de uno de los certificados del Carné Profesional, sino que se revocarán simultáneamente los tres certificados.

4.9.1 Causas para la revocación

Los certificados emitidos por la Autoridad de Certificación de la DGP pueden ser revocados por los siguientes motivos:

- Solicitud de Revocación formulada la persona física habilitada solicitante de un certificado electrónico de Sede electrónica o Sello.
- Sustracción, extravío, destrucción o deterioro del Carné Profesional soporte del Certificado.
- Tras la renovación por variación de los datos.
- Incapacidad sobrevenida, fallecimiento, perdida de la condición de funcionario o de su vinculación con la Dirección General de la Policía que permite la expedición del Carné Profesional
- Compromiso de las claves privadas del funcionario, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de la clave que permite la activación de dichas claves privadas, bien por cualquier otra circunstancia , incluidas las fortuitas, que indiquen el uso de las claves privadas por entidad ajena a su titular.
- Compromiso de la clave privada de la Autoridad de Certificación de la Dirección General de la Policía emisora del certificado del funcionario por cualquiera de las causas mencionadas en el punto anterior.
- Por incumplimiento por parte de la Autoridad de Certificación, de los funcionarios responsables de la expedición o del funcionario titular, 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 los certificados emitidos por la Autoridad de Certificación de la Dirección General de la Policía.
- Por el Cese en la actividad como prestador de servicios de certificación por la de la Dirección General de la Policía salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
- Por resolución judicial o administrativa que lo ordene conforme a derecho.

El funcionario no podrá revocar sus certificados por voluntad propia, dado que son inherentes a las labores de su cargo.

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 al funcionario mediante los procedimientos internos de notificación disponibles en la Dirección General de la Policía.
- A través de esta DPC se pone en conocimiento del personal al servicio de la Dirección General de la Policía que todos los procedimientos relacionados con el Carné Profesional que implican el cambio del soporte físico van acompañados de la revocación de los certificados que contiene dicho soporte.

4.9.2 Quién puede solicitar la revocación

Estará legitimado para solicitar la revocación de un certificado:

- El suscriptor a nombre del cual el certificado fue emitido, cuando concurra cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.
- Un tercero aceptante cuando tenga constancia demostrable que un certificado emitido por la Autoridad de Certificación de la Dirección General de la Policía ha sido empleado con fines fraudulentos.
- El propio Cuerpo Nacional de la Policía como Autoridad de Certificación cuando concurra cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.

4.9.3 Procedimiento de solicitud de revocación

La solicitud de revocación de los certificados de Sede y Sello se realizara por la persona física habilitada, mediante un procedimiento análogo al utilizado para la solicitud de su emisión, mediante el envío del formulario correspondiente.

Las solicitudes de revocación de los certificados del Carné Profesional se realizarán personalmente por el interesado ante cualquier equipo expedidor del Carné Profesional, del departamento de personal de su plantilla de destino.

Dado que el titular del Carné Profesional está obligado a la custodia y conservación del mismo, en los casos que el motivo de revocación sea la pérdida de validez del soporte (por pérdida, sustracción, destrucción o deterioro), el titular deberá comunicar inmediatamente tales hechos a la Dirección General de la Policía por los procedimientos y medios habilitados.

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 Dirección General de la Policía podrá solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho que recomiende emprender dicha acción.

4.9.4 Periodo de gracia de la solicitud de revocación

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

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

La solicitud de revocación de un certificado será 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 del estado de revocación de los certificados emitidos por la Autoridad de certificación de la Dirección general de la Policía es obligatoria. El procedimiento ordinario de comprobación de la validez de un certificado será la consulta al Servicio de Validación propio de la Dirección General de la Policía, el cual mediante el protocolo OCSP indicará el estado del certificado.

4.9.7 Frecuencia de emisión de CRLs

La PKI de la Dirección general de la Policía publicará una única CRL indirecta en el repositorio y estará disponible como medio para intercambiar información del estado de los certificados con el Servicio de Validación de la Dirección General de la Policía.

La PKI de la Dirección general de la Policía publicará una nueva CRL en su repositorio en el momento que se produzca cualquier revocación, y, en último caso, a intervalos de 23 horas (aunque no se hayan producido modificaciones en la CRL) para las generadas por ACs subordinadas y de 3 meses para las ARL generadas por la AC Raíz.

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

Según lo estipulado en 4.9.7

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

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

Los usuarios pueden consultar el estado de los certificados emitidos por la Autoridad de Certificación de la Dirección general de la Policía a través de la Autoridad de Validación que está disponible las 24 horas de los 7 días de la semana.

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

La suspensión de un certificado consiste en la revocación temporal del mismo. Es decir, mientras que el certificado esté suspendido, el número de serie de dicho certificado aparecerá en la correspondiente CRL indicándose como causa de revocación la suspensión del mismo.

La suspensión podrá ser realizada de oficio por la Dirección General de la Policía, en previsión de la ocurrencia de alguna de las causas de extinción definitiva de los certificados, contempladas en el apartado "4.9.1 *Causas para la revocación*".

4.9.14 Quién puede solicitar la suspensión

La solicitud de suspensión podrá ser solicitada por:

- El titular del certificado en previsión de la ocurrencia de alguna de las causas de extinción definitiva de los certificados, contempladas en el apartado "4.9.1 Causas para la revocación".
- El propio Cuerpo Nacional de la Policía como Autoridad de Certificación en las mismas circunstancias.

4.9.15 Procedimiento para la solicitud de suspensión

El procedimiento de solicitud de suspensión equivale al procedimiento descrito en el apartado 4.9.3 para la revocación de certificados.

4.9.16 Límites del periodo de suspensión

El certificado permanecerá suspendido durante el periodo de tiempo durante el cual se den las circunstancias descritas en el apartado 4.9.14, sin existir un plazo máximo.

Transcurrido este tiempo la Dirección General de la Policía decidirá la revocación definitiva del certificado o la activación del mismo.

4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1 Características operativas

Para la validación de los certificados emitidos por la Dirección General de la Policía se ofrecerá un servicio de validación que proporcionará información sobre el estado de dichos certificados emitidos.

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

Este sistema está disponible para la validación de los certificados por parte de los servicios propios de la Dirección General de la Policía, así como, para aquellos prestadores de servicios que confíen en dicha infraestructura de clave pública.

4.10.2 Disponibilidad del servicio

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

4.10.3 Características adicionales

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

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

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

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

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 Prácticas y políticas de custodia y recuperación de claves

No se ha establecido ningún procedimiento para la recuperación de las claves privadas asociadas a los certificados de Sede y Sello electrónico.

En el caso de los certificados del Carné Profesional, las claves privadas del certificado de Firma y del de Autenticación se generan dentro del Chip de la tarjeta soporte del Carné

Profesional, que al ser un dispositivo seguro de creación de firma, por diseño impide su exportación al exterior.

En cuanto a las claves de cifrado se generan de forma externa a la tarjeta en el momento de la expedición del Carné Profesional, para poder archivar la clave privada junto con su certificado. El formato de almacenamiento será PKCS#12. Este PKCS#12 estará protegido por una clave de acceso, o contraseña, la cual se generará en el momento de almacenamiento en el Servicio de Archivo y Recuperación de Claves de Cifrado.

El servicio de archivo y recuperación de claves de cifrado tendrá las siguientes funcionalidades:

- Almacenamiento de PKCS#12 y contraseña

  Esta funcionalidad permitirá durante la expedición del Carné Profesional realizar una copia de seguridad de la clave privada de cifrado y su certificado asociado. Esta información estará asociada al usuario, para que este pueda consultarla.

  Se almacenarán las claves de cifrado generadas durante la primera inscripción y las subsecuentes renovaciones, por lo que se mantendrá un historio de cada clave de cifrado.

- Consulta del histórico personal

  Esta funcionalidad permitirá a los usuarios del sistema recuperar las claves de cifrado, tanto actuales como antiguas en formato PKCS#12 cifrado, mediante una solicitud al Servicio de Archivo y Recuperación de Claves de Cifrado. El servicio autenticará al usuario, a través del certificado de autenticación, y le devolverá un menú de selección con sus PKCS#12 y las contraseñas asociadas a cada uno de ellos, permitiendo al usuario descargar el elemento seleccionado.

- Consulta del histórico ajeno

  Esta funcionalidad permitirá a ciertos usuarios del sistema recuperar claves de cifrado de otros usuarios, en formato de fichero PKCS#12 cifrado, mediante una solicitud al Servicio de Archivo y Recuperación de Claves de Cifrado. Existen dos grupos de usuarios un primer grupo a los que se permite la recuperación de los ficheros PKCS#12 y un segundo grupo compuesto por aquellos que tienen autorizada la recuperación de las contraseñas asociadas a cada uno de los ficheros PKCS#12.

  Este servicio permitirá seleccionar la clave que se desea recuperar. La petición de recuperación se ejecutara en dos pasos, verificando que haya transcurrido el tiempo mínimo de seguridad entre ambos pasos (el tiempo mínimo entre accesos será configurable y nunca menor de 24 horas). Se autenticará al usuario y se verificarán sus privilegios de acceso a esta información. Tras estas validaciones, en caso positivo le devolverá un fichero que contendrá el PKCS#12 o la password asociada al mismo.

  Los usuarios autorizados para realizar esta gestión son:

  - Autorizados a acceder al fichero PKCS#12:
    - Los responsables de las Comisarias Generales de la Dirección General de la Policía. En la actualidad:
      - Comisario General de Información.
      - Comisario General de Policía Judicial.
      - Comisario General de Seguridad Ciudadana.

- Comisario General de Extranjería y Fronteras.
- Comisario General de Policía Científica.

o Autorizados a acceder a la contraseña del fichero PKCS#12:

- Los responsables de las Divisiones de la Dirección General de la Policía. En la actualidad:
  - Jefe de la División de Personal.
  - Jefe de la División de Formación y Perfeccionamiento.
  - Jefe de la División Económica y Técnica.
  - Jefe de la División de Documentación

Respecto a las claves de autenticación y firma, la tarjeta soporte del Carné Profesional es un dispositivo de creación de firma, y las claves generadas internamente no pueden ser exportadas en ningún caso.

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

No estipulado.

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

5.1 CONTROLES FÍSICOS

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

5.1.1 Ubicación física y construcción

El edificio donde se encuentra ubicada la infraestructura del Carné Profesional dispone de medidas de seguridad de control de acceso, de forma que sólo se permite la entrada al mismo a las personas debidamente autorizadas.

Todas las operaciones críticas relacionadas con el Carné Profesional 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 Dirección General de la Policía, de forma que sólo el personal autorizado pueda acceder a ellos.

EL Centro de Proceso de Datos de la Dirección General de la Policía cumplen los siguientes requisitos físicos:

a) Está alejado 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 del Carné Profesional estarán físicamente separados de otros sistemas de la Dirección General de la Policía 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 del Carné Profesional 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 Carné Profesional 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

La Dirección General de la Policía ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva.

La Dirección General de la Policía 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

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

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

5.2.1 Roles responsables del control y gestión de la PKI

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

- **Administradores de Sistema**: Conjunto de usuarios autorizados a realizar ciertas tareas relacionadas con la instalación, configuración y mantenimiento de las entidades de la PKI, pero con acceso limitado a la información relacionada con los parámetros de seguridad. Responsable del funcionamiento de los sistemas que componen la PKI, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de batos, 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 logs de auditoría de las entidades de la PKI.
- **Coordinador de Seguridad**: responsable de la definición y verificación de todos los procedimientos de seguridad tanto física como informática.

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

5.2.2 Número de personas requeridas por tarea

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

5.2.3 Identificación y autenticación para cada usuario

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

El resto de usuarios autorizados de la PKI de la Dirección General de la Policía se identifican mediante certificados electrónicos emitidos por la propia infraestructura alojados en tarjetas criptográficas.

La autenticación se complementa con las correspondientes autorizaciones para acceder a determinados activos de información o sistemas de la Dirección General de la Policía.

5.2.4 Roles que requieren segregación de funciones

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

- Incompatibilidad entre el rol auditor (i.e. auditor de sistema) y cualquier otro rol.
- Incompatibilidad entre los roles administrativos (coordinador de seguridad, administrador de sistema y oficial de registro)
- Incompatibilidad entre los administradores y los operadores del HSM

- Incompatibilidad entre el oficial de seguridad y el administrador del HSM

5.3 CONTROLES DE PERSONAL

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

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

Para ello, la Dirección General de la Policía 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 Dirección General de la Policía.

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 Dirección General de la Policía.

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 de la Infraestructura de Clave Pública de la Dirección General de la Policía de forma inmediata al conocimiento del hecho.

5.3.7 Requisitos de contratación de terceros

Se aplicará la normativa general de la Dirección General de la Policía para las contrataciones.

5.3.8 Documentación proporcionada al personal

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

5.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.4.1 Tipos de eventos registrados

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

- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware.
- Mantenimiento del sistema.
- Cambios de personal

- Cambios en las claves de la Autoridad de certificado
- Cambios en las políticas de emisión de certificados y en la presente DPC
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor
- Informes de compromisos y discrepancias
- Registros de acceso físico
- Acontecimientos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste
- La ceremonia de generación de claves y las bases de datos de gestión de claves

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

Categoría: Indica la importancia del evento.

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

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

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

Rol: Tipo de Autoridad que generó el evento.

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

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

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

Descripción: Representación textual del evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyos valores variarán dependiendo de los datos sobre los que se ejecutó la operación. Algunos ejemplos de los parámetros que se incluyen para la descripción del evento “Certificado

generado" son: el número de serie, el nombre distintivo del titular del certificado emitido y la plantilla de certificación que se ha aplicado.

5.4.2 Frecuencia de procesado de registros de auditoría

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

5.4.3 Periodo de conservación de los registros de auditoría

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

5.4.4 Protección de los registros de auditoría

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

Las copias de backup de dichos registros se almacenan en un archivo ignífugo cerrado dentro de las instalaciones seguras de la Dirección General de la Policía.

La destrucción de un archivo de auditoría solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorías de la Infraestructura de Clave Pública de la Dirección General de la Policía. 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 como mínimo 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 Dirección General de la Policía 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 la Infraestructura de Clave Pública de la Dirección General de la Policía.

Todos los elementos significativos existentes en la Infraestructura de Clave Pública de la Dirección General de la Policía se acumulan en una Base de Datos. Los procedimientos de control de seguridad empleados en la Infraestructura de Clave Pública de la Dirección General de la Policía se basan en la tecnología de construcción empleada en la base de datos.

Las características de este sistema son las siguientes:

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

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

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

5.4.7 Notificación al sujeto causa del evento

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

5.4.8 Análisis de vulnerabilidades

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

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

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

5.5 ARCHIVO DE REGISTROS

5.5.1 Tipo de eventos archivados

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

Las operaciones registradas incluyen las realizadas por los administradores que utilizan las aplicaciones de administración de los elementos de la Infraestructura de Clave Pública, 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 de la PKI están protegidos mediante técnicas criptográficas, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.

La destrucción de un archivo de Registro solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Coordinador de Seguridad y el Administrador de Auditorías de la Infraestructura de Clave Pública de la Dirección General de la Policía. 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 Dirección General de la Policía para las copias de respaldo del resto de sistemas de información de la Dirección General de la Policía.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de información empleados por la Infraestructura de Clave Pública de la Dirección General de la Policía 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 la Infraestructura de Clave Pública están sincronizados en fecha y hora. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (Network Time Protocol) se autocalibran a través de la Red Interministerial (en la actualidad red SARA de Sistema de Aplicaciones y Redes para las Administraciones), utilizando como referencia la establecida oficialmente en España (en la actualidad 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 Dirección General de la Policía.

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 los sitios web https://sede.policia.gob.es y www.policia.es y en la Orden General de la Dirección General de la Policía (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 el apartado 4.7 del presente 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 Dirección General de la Policía tiene establecido un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los

servicios de certificación prestados por la infraestructura de Clave Pública de la Dirección General de la Policía.

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

- La redundancia de los componentes más críticos.
- El chequeo completo y periódico de los servicios de copia de respaldo.

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

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 restablezca 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 de Certificación se procederá a su revocación inmediata. Seguidamente, se generará y publicará la correspondiente ARL, cesando en su funcionamiento dicha Autoridad.

El certificado revocado de la misma permanecerá accesible en el repositorio de la infraestructura de Clave Pública de la Dirección General de la Policía con objeto de continuar verificando los certificados emitidos durante su periodo de funcionamiento. La notificación de la revocación se hará efectiva a través de los sitios Web https://sede.policia.gob.es y www.policia.es y en la Orden General (ver apartado 2.1)

Las Autoridades de Certificación componentes de la infraestructura de Clave Pública de la Dirección General de la Policía dependientes de la AC afectada serán informadas del hecho y conminadas a solicitar una nueva certificación por otra AC de dicha infraestructura.

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 revocación.

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

La infraestructura de Clave Pública de la Dirección General de la Policía puede ser reconstruida en caso de desastre. 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 la infraestructura de Clave Pública de la Dirección General de la Policía.
- 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 ultima 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 el sistema en producción y en los elementos de recuperación.

5.8 CESE DE UNA AC O AR

5.8.1 Autoridad de Certificación

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

En caso de cese de la actividad de una o de todas sus ACs, se comunicará a los titulares de sus certificados, a través de los sitios web https://sede.policia.gob.es y www.policia.es y de la Orden General y con un plazo mínimo de antelación de 2 meses al citado cese de actividad, su intención de que la/s AC correspondientes cesen en la actividad como prestadores de servicios de certificación.

En el supuesto de que la Dirección General de la Policía decidiera transferir la actividad de Prestador de Servicios de Certificación a otro organismo, comunicará a los titulares de sus certificados los acuerdos de transferencia. A tal efecto la Dirección General de la Policía enviará un documento explicativo de las condiciones de transferencia y de las características del Prestador al que se propone la transferencia de la gestión de los certificados. Esta comunicación se realizará por cualquier medio que garantice el envío y

la recepción de la notificación, con una antelación mínima de 2 meses al cese efectivo de su actividad.

La Dirección General de la Policía comunicará al Organismo Ministerial competente (en la actualidad el Ministerio de Industria, Energía y Turismo), con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados especificando si va a transferir la gestión y a quién o si se extinguirá su vigencia.

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

La Dirección General de la Policía remitirá al Organismo Ministerial competente (en la actualidad el Ministerio de Industria, Energía y Turismo) con carácter previo al cese definitivo de su actividad la información relativa a los certificados cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a los efectos previstos en el artículo 20.1.f de la Ley de Firma electrónica.

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

5.8.2 Autoridad de Registro

No procede

6. CONTROLES DE SEGURIDAD TÉCNICA

La infraestructura de Clave Pública de la Dirección General de la Policía utiliza sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 Generación del par de claves

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

La clave privada de los certificados de sede electrónica o sello se genera en el interior del servidor en el que se instalará dicho certificado.

En los certificados del Carné Profesional:

- Las claves para los certificados de autenticación y firma emitidos por la AC *Subordinada* se generan en la propia tarjeta criptográfica del titular, la cual cumple los requisitos de Dispositivo de Creación de Firma.
- Las claves de cifrado se generarán en un dispositivo hardware específico para la creación de las claves de cifrado. Este hardware criptográfico está normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3 o superior nivel de seguridad.

6.1.2 Entrega de la clave privada al titular

La clave privada de los certificados de sede electrónica o sello se genera en el interior del servidor en el que se instalará los certificados. En aquellos casos en que no sea posible su generación interna, la clave privada será generada por el departamento policial competente (en la actualidad el Área de Informatica) y se le enviará al solicitante mediante un correo electrónico cifrado y con acuse de recibo.

En los certificados del Carné Profesional:

- Las claves privadas de autenticación y firma se generan 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.

- La clave privada de cifrado se genera en el backend utilizando un dispositivo criptográfico HSM para permitir su almacenamiento y recuperación en caso de pérdida. Dicha clave se transmite de forma segura al puesto de expedición, se almacena en la tarjeta quedando configurada como no exportable con el mismo nivel de seguridad que los otros dos pares de claves.

6.1.3 Entrega de la clave publica al emisor del certificado

La clave publica de los certificados de sede electrónica o sello que se genera en el interior del servidor se enviará al departamento policial competente (en la actualidad el Área de Informatica) mediante un paquete PKCS#10. En aquellos casos en que no sea posible su generación interna, la clave pública será generada por el citado departamento policial competente (en la actualidad el Área de Informatica).

En los certificados del Carné Profesional:

- 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 de la DGP formando parte de una solicitud de certificación en formato PKIX-CMP.

- Las claves de cifrado son generadas externamente en un dispositivo criptográfico (HSM). La clave pública es enviada a la AC subordinada en un mensaje PKIX-CMP, junto con las otras solicitudes de certificación correspondientes a las claves de firma y de autenticación.

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

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

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

El certificado de la AC raíz de la infraestructura de Clave Pública de la Dirección General de la Policía, 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 que aparecerá publicada en los sitios web https://sede.policia.gob.es y www.policia.es y en la Orden General.

6.1.5 Tamaño de las claves

El tamaño de las claves de la AC Raíz se establece de acuerdo con el parámetro TC-AC-R (que en la actualidad es de 4096 bits).

El tamaño de las claves de las AC Subordinadas se establece de acuerdo con el parámetro TC-AC-S (que en la actualidad es de 2048 bits).

El tamaño de las claves de los certificados de Sede electrónica y de Sello se establece de acuerdo con el parámetro TC-C-SS (que en la actualidad será como mínimo de 2048 bits).

El tamaño de las claves de los certificados del Carné Profesional se establece de acuerdo con el parámetro TC-C-CP (que en la actualidad es de 2048 bits).

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

La clave pública de la AC Raíz y de la AC Subordinada está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

La clave pública de los certificados emitidos por la PKI de la DGP 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 el informe especial del ETSI SR 002 176, que indica la calidad de los algoritmos de firma electrónica. Los algoritmos y parámetros de firma utilizados por las Autoridades de Certificación de la infraestructura de Clave Pública de la Dirección General de la Policía 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

TC-AC-R bits para AC Raíz / TC-AC-S bits para ACs Subordinadas

Algoritmo de generación de claves: rsagen1

Método de relleno: emsa-pkcs1-v1_5

Funciones criptográficas de Resumen: Estas funciones se establecen de acuerdo con el Parámetro FCR (que en la actualidad es: SHA-1/SHA-256).

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

Los usos admitidos de la clave para cada tipo de certificado emitido por la infraestructura de Clave Pública de la Dirección General de la Policía vienen definidos por la Política de Certificación que le sea de aplicación.

Todos los certificados emitidos por la infraestructura de Clave Pública de la Dirección General de la Policía 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 la Dirección General de la Policía.

A tal efecto, en los campos 'Key Usage' de los certificados asociados a la infraestructura de Clave Pública de la Dirección General de la Policía se han incluido los siguientes usos:

- A la Sede Electrónica. O.I.D. (2.16.724.1.2.1.102.34/35)

KEY USAGE	EXTENDED KEY USAGE
Digital Signature, Key Encipherment	Authentication TSL Web Server

- Al Sello Electrónico. O.I.D. (2.16.724.1.2. 1.102.36/37)

KEY USAGE	EXTENDED KEY USAGE
Digital Signature, Key Encipherment Content Commitment Data Encipherment	Email Protection: Protección de mail Client Authentication: Autenticación deCliente

- Al Carne Profesional:

CERTIFICADO	KEY USAGE	EXTENDED KEY USAGE
Certificado de Firma (2.16.724.1.2. 1.102.30)	contentCommitment[4]	
Certificado de Autenticación (2.16.724.1.2. 1.102.31)	Digital Signature	Autenticación del cliente Inicio de sesión de tarjeta inteligente Cualquier propósito Correo seguro
Certificado de Cifrado (2.16.724.1.2. 1.102.32)	Key Encipherment, Data Encipherment	Correo seguro Cualquier propósito Sistema de cifrado de archivos

[4] Nonrepudiation

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

6.2.1 Estándares para los módulos criptográficos

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

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

a) Inicialización del estado del módulo HSM.

b) Creación de las tarjetas de administración y de operador.

c) Generación de las claves de la AC.

En cuanto a las tarjetas criptográficas con certificados para firma electrónica avanzada, aptas como dispositivos de creación de firma, soportan los estándares PKCS#11 y CSP.

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

La clave privada, tanto de la AC Raíz como de AC *Subordinada*, se encuentra bajo control multipersona[5]. Ésta se activa mediante la inicialización del software de AC por medio de una combinación de operadores de la AC, administradores del HSM y usuarios de S.O.. Éste es el único método de activación de dicha clave privada.

La clave privada de los certificados de sede electrónica o sello están bajo el exclusivo control del titular de los certificados.

En el caso de los certificados del Carné Profesional:

- Las claves privadas de los certificados de autenticación y firma, están bajo el control exclusivo del titular del Carné Profesional.
- La clave privada de los certificados de cifrado se encuentra almacenada en el Servicio de Archivo y Recuperación de Claves y sólo es accesible por el propio titular o por personal autorizado

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

6.2.3 Custodia de la clave privada

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

La clave privada de los certificados de sede electrónica o sello están bajo el exclusivo control del titular de los certificados siendo estos responsables de su custodia.

En el caso de los certificados del Carné Profesional:

- La custodia de las claves privadas de los certificados de firma y autenticación la realizan los funcionarios titulares de las mismas. En ningún caso la AC guarda copia de la clave privada de firma y autenticación ya que ésta no puede ser extraída de la tarjeta.
- Las claves privadas correspondientes a los certificados de cifrado son generadas de manera centralizada. Una vez generada el certificado y la clave privada de cifrado, se almacenan en la tarjeta y en un repositorio de claves. Las claves privadas de cifrado almacenadas en el repositorio de claves sólo podrán ser accedidas por el usuario propietario de clave o personal autorizado.

Las claves privadas del funcionario se encuentran almacenadas en el procesador de la tarjeta criptográfica del Carné Profesional. Con esto se consigue que las claves privadas no abandonen nunca el soporte físico, tanto las generadas internamente como la importada, minimizando las posibilidades de comprometer dichas claves.

Para el acceso a las claves, el titular del Carné Profesional deberá emplear una clave personal de acceso (PIN). Este PIN, tras la expedición del CP, tomará como valor inicial el DNI/NIE y la letra de este. El titular del CP deberá asignar al PIN otro valor de su exclusivo conocimiento con las herramientas que el Area de Informática proporcione para este propósito.

Así mismo se generará un código de desbloqueo (PUK) que podrá ser utilizado en caso de bloqueo de la tarjeta, tras presentar un PIN erróneo un número determinado de veces. Este código de desbloqueo se almacenará en un repositorio que podrá ser consultado por el usuario en cualquier momento, previa autenticación a dicho servicio de archivo. La autenticación se realiza a través del Servicio de Gestión de Accesos, haciendo uso del certificado de autenticación contenido en el Carné Profesional, o en caso de no disponer de dicho Carné, tendrá la posibilidad de autenticarse mediante usuario/contraseña.

El funcionario podrá modificar su clave personal de acceso 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 presentación del código de desbloqueo – PUK, correspondiente.

  Este código de desbloqueo será entregado al funcionario junto con su Carné Profesional En caso de la pérdida del código de desbloqueo, sólo el usuario asociado podrá recuperarlo autenticándose al repositorio de claves.

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

6.2.4 Copia de seguridad de la clave privada

Las claves privadas de las ACs del sistema de la infraestructura de Clave Pública de la Dirección General de la Policía 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.

Este apartado no aplica para los certificados de sede electrónica o sello.

En el caso de los certificados del Carné Profesional:

- No es posible realizar una copia de seguridad de las claves privadas asociadas a los certificados del Carné Profesional (autenticación y firma electrónica) ya que las claves no pueden ser exportadas de las tarjetas y éstas no son clonables.
- Durante el proceso de expedición del Carné Profesional, la clave privada de cifrado se almacena en un repositorio de claves para que, en caso de inutilizarse el acceso desde la tarjeta, sea posible el descifrado de la información cifrada con dicha clave.

6.2.5 Archivo de la clave privada

Las claves privadas de la ACs de la infraestructura de Clave Pública de la Dirección General de la Policía 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.

Este apartado no aplica para los certificados de sede electrónica o sello.

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

Las claves privadas asociadas a los certificados de cifrado de los titulares del Carné Profesional son archivadas para su permitir su posterior recuperación, en el Servicio de Archivo y Recuperación de Claves de cifrado, sólo por el propietario de la clave o por personal autorizado según el procedimiento descrito en otros apartados de este documento.

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

La transferencia de la clave privada de las ACs de la infraestructura de Clave Pública de la Dirección General de la Policía 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.

Este apartado no aplica para los certificados de sede electrónica o sello.

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

Las claves privadas de cifrado se generan en un dispositivo criptográfico externo y se inyectan en la tarjeta a través de un canal seguro (autenticado y cifrado). Esta operativa sólo puede realizarse desde un puesto autorizado de una Oficina de Expedición.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en el módulo criptográfico en el momento de la creación de cada una de las Autoridades de la infraestructura de Clave Pública de la Dirección General de la Policía que hacen uso de dichos módulos.

Este apartado no aplica para los certificados de sede electrónica o sello

La tarjetas soporte del Carné Profesional son dispositivos de creación de firma. Las claves privadas asociadas a la identidad y firma del funcionario se crean en la tarjeta criptográfica en presencia del mismo y en ningún caso es posible su extracción y/o exportación a otro dispositivo.

6.2.8 Método de activación de la clave privada

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

La clave privada de los certificados de sede electrónica o sello están bajo el exclusivo control del titular de los certificados que deberá activarlas introduciendo el PIN o clave de acceso correspondiente a cada certificado.

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

6.2.9 Método de desactivación de la clave privada

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

Para la desactivación de las claves de los Certificados de Sede o Sello será necesario realizar una parada del Servidor o servicio donde este alojado dicho certificado. Para su reactivación será necesario volver a introducir el PIN o clave de acceso correspondiente a cada certificado tras reiniciar el servicio o servidor al que este asociado.

Las claves privadas asociadas a los certificados del Carné Profesional se pueden desactivar retirando la tarjeta del lector o pasado un tiempo establecido tras la introducción de la clave personal de acceso -PIN. Este tiempo de "cacheo" del PIN se establece en 5 min para las claves de autenticación y cifrado. El PIN para las claves de firma no se cachea, siendo necesario la introducción del PIN para activar las claves cada vez que se vaya a hacer uso de las mismas.

6.2.10 Método de destrucción de la clave privada

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

En el caso de las ACs de la infraestructura de Clave Pública de la Dirección General de la Policía, la destrucción consistiría en el borrado seguro de las claves de los HSM que las albergase, así como de las copias de seguridad.

Para las claves de los certificados de Sede Electrónica y Sello se procederá igualmente a la destrucción segura de dichas claves.

En el caso de los certificados asociados al Carne Profesional, la destrucción de la clave privada:

- Se realizará en los procesos de renovación de dicha clave cuando no medie una renovación del soporte del Carné Profesional.
- Irá acompañada de la inutilización física de la tarjeta que la alberga, cuando se renueve el soporte del Carné Profesional, por las causas descritas en apartados anteriores, cuando se deteriore la tarjeta de tal forma que no permita un uso eficiente de la misma.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 Archivo de la clave pública

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

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

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

El certificado y el par de claves de AC Raíz del sistema de la infraestructura de Clave Pública de la Dirección General de la Policía 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 certificación.

La caducidad de los certificados emitidos por la infraestructura de Clave Pública de la Dirección General de la Policía ocurrirá en un máximo de TV-C-CP meses (36 meses en la actualidad) meses a contar desde el momento de su expedición.

Para los funcionarios de la Dirección General de la Policía, el Carné Profesional se ha definido el siguiente criterio de periodo de validez:

- El soporte físico no tendrá especificada una fecha de caducidad. El Carné Profesional será válido mientras sus titulares ostenten la misma categoría y situación administrativa que en el momento de la expedición, debiendo procederse por la Administración a la retirada de los mismos cuando varíe alguna de ellas.

Para el personal que presta servicios o se halla vinculado a la Dirección General de la Policía, los documentos identificativos profesionales tendrán la siguiente validez:

- Las personas que ostenten la titularidad de los Órganos Directivos, el Carné Profesional será válido mientras desempeñen la titularidad de dichos órganos.
- Los alumnos del centro de formación para ingreso y funcionarios en prácticas de la Dirección General de la Policía, el Carné Profesional será válido durante el tiempo que ostenten tal condición.
- Los funcionarios de los Cuerpos de la Administración General del Estado o de otras Administraciones Públicas y personal laboral que desempeñen puestos de trabajo en la Dirección General de la Policía, el Carné Profesional será válido en tanto desempeñen el puesto de trabajo que dio lugar a la expedición.

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

La caducidad de un certificado del Carné Profesional inhabilita el uso legítimo por parte de su titular.

6.4 DATOS DE ACTIVACIÓN

6.4.1 Generación e instalación de los datos de activación

Para la instauración de una Autoridad de Certificación del dominio de la Dirección General de la Policía 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.

Para los certificados de sede electrónica o sello, el dato de activación consiste en el PIN o clave de acceso que se introduce en el momento de la generación de las claves, siendo el titular de los certificados el responsable de que permanezca bajo su exclusivo control y conocimiento.

En el caso de las claves asociadas a los certificados del Carné Profesional, de autenticación, firma electrónica y cifrado del funcionario, 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 funcionario en el momento en que se generan las claves y permanece bajo su exclusivo conocimiento durante todo el ciclo de vida de las claves.

6.4.2 Protección de los datos de activación

Sólo el personal autorizado, en este caso los Operadores y Administradores 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.

La clave privada de los certificados de sede electrónica o sello están bajo el exclusivo control del titular de los certificados siendo este el responsable de la protección de las claves privadas del certificado y de los datos de activación de los mismos

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

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

- Memorícelo y procure no anotarlo en ningún documento físico ni electrónico que el titular conserve o transporte junto con el Carné Profesional, fundamentalmente si existe posibilidad de que se pierda o se robe al mismo tiempo que aquella.
- No envíe ni comunique su PIN a nadie ni por ningún medio, ya sea vía telefónica, correo electrónico, etc.
- Recuerde que el PIN es personal e intransferible. Si cree que su PIN puede ser conocido por otra persona, debe cambiarlo. El uso del PIN 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 del PIN, 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/NIE, etc.)
- Se recomienda cambiar el PIN de acceso periódicamente.

6.4.3 Otros aspectos de los datos de activación

En el caso de las claves asociadas a los certificados del Carné Profesional, éste podrá modificar, mediante un software disponible en su PC, los datos de activación (clave personal de acceso –PIN-) siempre que permanezcan bajo su conocimiento, esto es, no hayan sido olvidados o se haya bloqueado la tarjeta debido a intentos de acceso fallidos con datos de activación incorrectos.

El funcionario podrá realizar el cambio de PIN o desbloqueo de la tarjeta haciendo uso código de desbloqueo (PUK) proporcionado durante de la generación del Carné Profesional. El código de desbloqueo también estará disponible, sólo para el funcionario y en caso de extravío, a través de los mecanismos ofrecidos por la aplicación de recuperación de claves.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionaran a quien acredite la necesidad de conocerlos y la Habilitación Personal de Seguridad correspondiente. Esto será aplicable tanto para los casos de auditorías, externas o internas, como para las labores de inspección que deban realizar los diferentes órganos de control o supervisión.

6.5.1 Requerimientos técnicos de seguridad específicos

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

Asimismo, respecto de la gestión de la seguridad de la información, se sigue el esquema previsto en UNE-ISO/IEC 27002:2009 Código de Buenas Prácticas para la Seguridad de la Información.

6.5.2 Evaluación de la seguridad informática

Los procesos de gestión de la seguridad de la infraestructura de Clave Pública de la Dirección General de la Policía 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.

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

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

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

6.6.1 Controles de desarrollo de sistemas

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición de sistemas informáticos como en el desarrollo de los mismos ya que pueden tener algún impacto sobre la seguridad la infraestructura de Clave Pública de la Dirección General de la Policía

Se realiza un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente utilizado en las aplicaciones que constituyen cada uno de sistemas la infraestructura de Clave Pública de la Dirección General de la Policía, 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 de Clave Pública de la Dirección General de la Policía está dotada de los entornos de desarrollo y producción claramente diferenciados e independientes.

6.6.2 Controles de gestión de seguridad

La organización encargada del sistema de la infraestructura de Clave Pública de la Dirección General de la Policía, mantiene un inventario de todos los activos informáticos y realizará una clasificación de los mismos de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

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

6.6.3 Controles de seguridad del ciclo de vida

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan algún impacto en la seguridad de la infraestructura de Clave Pública de la Dirección General de la Policía.

6.7 CONTROLES DE SEGURIDAD DE LA RED

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

No obstante indicar que, la infraestructura de la red utilizada por el sistema de la infraestructura de Clave Pública de la Dirección General de la Policía está dotada de todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro (p.e.

utilización de cortafuegos o intercambio de datos cifrados entre redes). Esta red también es auditada periódicamente.

6.8 FUENTES DE TIEMPO

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

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

Todos los sistemas que constituyen la infraestructura de Clave Pública de la Dirección General de la Policía están sincronizados en fecha y hora, a través de la Red Interministerial (en la actualidad red SARA del Sistema de Aplicaciones y Redes para las Administraciones), utilizando como fuente segura de tiempos la establecida oficialmente en España (en la actualidad la proporcionada por el Real Instituto y Observatorio de la Armada.

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 PERFIL DE CERTIFICADO

Los certificados emitidos por la infraestructura de Clave Pública de la Dirección General de la Policía serán conformes con las siguientes normas:

- RFC 5280 (2008-05): Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004
- RFC 3739 (2004-03): Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, (prevaleciendo en caso de conflicto la TS 101 862).

Se ha adoptado el criterio de que todos los elementos de tipo *Directory String* contenidos en los campos *Issuer* y *Subject* estarán codificados en UTF8, a excepción de aquellos que tienen explícitamente una codificación distinta, como son los campos *C* y *SerialNumber,* que irán codificados en *PrintableString*.

7.1.1 Número de versión

Todos los certificados expedidos por la Infraestructura de Clave Pública de la Dirección General de la Policía utilizan el estándar X.509 versión 3 (X.509 v3)

7.1.2 Extensiones del certificado

Los certificados asociados al Carné Profesional vinculan la identidad de una persona física (Nombre, Apellidos y número del Documento Nacional de Identidad) a una determinada clave pública, incluyendo ciertos atributos asociados a dicha entidad. Para garantizar la autenticidad y no repudio, toda esta información estará firmada electrónicamente por la institución encargada de la emisión del Carné Profesional.

Los datos personales del funcionario incluidos en el certificado son:

- Nombre y apellidos
- Número del Documento Nacional de Identidad
- Clave pública asociada
- Número del Carné Profesional
- Cargo que desempeña dentro de la Dirección General de la Policía
- Dirección de correo electrónico
- UPN - *User Principal Name*: identificador de usuario, en el Directorio Activo de la Dirección General de la Policía

Las extensiones utilizadas en los certificados son:

- *KeyUsage*. Calificada como crítica.
- *BasicConstraint*. Calificada como crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *Auth. Information Access*
- *Subject Altenative Name*
- *qcstatements*

A continuación se recogen los perfiles de los tres tipos de certificados emitidos al personal al servicio de la Dirección General de la Policía.

Certificado de No Repudio		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	

Certificado de No Repudio		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption[6] sha1withRsaEncryption)	
4. Issuer Distinguished Name	CN=AC DGP XXX[7] OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	Máximo 36 meses	
6. Subject	CN=NOMBRE APELLIDO1 APELLIDO2 – DNI /NIE (con letra) (FIRMA) GIVENNAME= NOMBRE SURNAME= APELLIDO1 APELLIDO2 - DNI/NIE (con letra) SERIALNUMBER= DNI/NIE (con letra) OU=AMBITO DEL CUERPO NACIONAL DE POLICIA OU=EMPLEADO PUBLICO O=MINISTERIO DE INTERIOR C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	0	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	No se utilizará	

[6] Se utilizara *sha1withRsaEncryption* para la garantizar la compatibilidad con las aplicaciones y sistemas que actualmente no soportan *sha256withRsaEncryption*.

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

Certificado de No Repudio		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.1.102.30 OID asociado a la PC de certificado de no repudio de funcionario.	
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod: 15 años	NO
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*. Tipo=EMPLEADO PUBLICO. OID: 2.16.724.1.3.5.3.1.1 - *entidad*. Entidad Suscriptora=MINISTERIO DE INTERIOR. OID: 2.16.724.1.3.5.3.1.2 - *nif entidad.* NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.3.1.3 - *dni*. DNI/NIE. OID: 2.16.724.1.3.5.3.1.4 - número identificación. Número identificativo=NIP. OID:2.16.724.1.3.5.3.1.5 - *nombre*. N= NOMBRE. OID: 2.16.724.1.3.5.3.1.6 - *apellido1*. SN1=APELLIDO1. OID: 2.16.724.1.3.5.3.1.7 - apellido*2*. SN2=APELLIDO2. OID: 2.16.724.1.3.5.3.1.8 - correo electrónico. OID: 2.16.724.1.3.5.3.1.9 - *puesto* (RFC 5282). Puesto=CARGO. OID: 2.16.724.1.3.5.3.1.11. (Opcional) - *upn*=UPN. (Opcional)	NO
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	
11. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es) CA: URL-AC-R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	

Certificado de No Repudio		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

Certificado de Autenticación		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption sha1withRsaEncryption)	
4. Issuer Distinguished Name	CN=AC DGP XXX OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	Máximo 36 meses	
6. Subject	CN=NOMBRE APELLIDO1 APELLIDO2 – DNI /NIE (con letra) (AUTENTICACION) GIVENNAME= NOMBRE SURNAME= APELLIDO1 APELLIDO2 - DNI/NIE (con letra) SERIALNUMBER= DNI/NIE (con letra) OU=AMBITO DEL CUERPO NACIONAL DE POLICIA OU=EMPLEADO PUBLICO O=MINISTERIO DE INTERIOR C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)

Certificado de Autenticación		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	*Client/auth (1.3.6.1.5.5.7.3.2)* *SmartCardLogon (1.3.6.1.4.1.311.20.2.2)* *Secure Email (1.3.6.1.5.5.7.3.4)* *anyExtendedKeyUsage (2.5.29.37.0)*	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.1.102.31 OID asociado a la PC de certificado de autenticación de funcionario.	
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod: 15 años	NO
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*. Tipo=EMPLEADO PUBLICO. OID: 2.16.724.1.3.5.3.1.1 - *entidad*. Entidad Suscriptora=MINISTERIO DE INTERIOR. OID: 2.16.724.1.3.5.3.1.2 - *nif entidad.* NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.3.1.3 - *dni*. DNI/NIE. OID: 2.16.724.1.3.5.3.1.4 - número identificación. Número identificativo=NIP. OID:2.16.724.1.3.5.3.1.5 - *nombre*. N= NOMBRE. OID: 2.16.724.1.3.5.3.1.6 - *apellido1*. SN1=APELLIDO1. OID: 2.16.724.1.3.5.3.1.7 - apellido*2*. SN2=APELLIDO2. OID: 2.16.724.1.3.5.3.1.8 - correo electrónico. OID: 2.16.724.1.3.5.3.1.9 - *puesto* (RFC 5282). Puesto=CARGO. OID: 2.16.724.1.3.5.3.1.11. (Opcional)	NO

Certificado de Autenticación		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
	- *upn*=UPN. (Opcional)	
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	
11. Basic Constraints		
Subject Type	Entidad Final	SI
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es) CA: URL-AC_R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

Certificado de Cifrado		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption sha1withRsaEncryption)	
4. Issuer Distinguished Name	CN=AC DGP XXX OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	Máximo 36 meses	
6. Subject	CN=NOMBRE APELLIDO1 APELLIDO2 – DNI /NIE (con letra) (CIFRADO) GIVENNAME= NOMBRE SURNAME= APELLIDO1 APELLIDO2 - DNI/NIE (con letra) SERIALNUMBER= DNI/NIE (con letra) OU=AMBITO DEL CUERPO NACIONAL DE POLICIA OU=EMPLEADO PUBLICO O=MINISTERIO DE INTERIOR C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		

Certificado de Cifrado		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	*s/mime* (1.3.6.1.5.5.7.3.4) *EFS* (1.3.6.1.4.1.311.10.3.4) *anyExtendedKeyUsage* (2.5.29.37.0)	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.1.102.32 OID asociado a la PC de certificado de cifrado de funcionario.	
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod: 15 años	NO
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*. Tipo=EMPLEADO PUBLICO. OID: 2.16.724.1.3.5.3.1.1 - *entidad*. Entidad Suscriptora=MINISTERIO DE INTERIOR. OID: 2.16.724.1.3.5.3.1.2 - *nif entidad.* NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.3.1.3 - *dni*. DNI/NIE. OID: 2.16.724.1.3.5.3.1.4 - número identificación. Número	NO

Certificado de Cifrado		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
	identificativo=NIP. OID:2.16.724.1.3.5.3.1.5 - *nombre*. N= NOMBRE. OID: 2.16.724.1.3.5.3.1.6 - *apellido1*. SN1=APELLIDO1. OID: 2.16.724.1.3.5.3.1.7 - apellido*2*. SN2=APELLIDO2. OID: 2.16.724.1.3.5.3.1.8 - correo electrónico. OID: 2.16.724.1.3.5.3.1.9 - *puesto* (RFC 5282). Puesto=CARGO. OID: 2.16.724.1.3.5.3.1.11. (Opcional)	
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	
11. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es) CA: URL-AC-R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

Los certificados del Carné Profesional se emiten en calidad de certificados reconocidos y, por tanto todos perfiles contienen los campos que establece la normativa legalmente aplicable en materia de Certificados Reconocidos:

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

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

Requisitos Legales	Modo de cumplimiento
La indicación que se expiden como certificados reconocidos (artículo 11.2.a 59/2003)	Inclusión de la extensión Qualified Certificate Statements que incorpora las siguientes declaraciones: 1.- id-etsi-qcs-QcCompliance – Indica que el certificado se emite como reconocido de acuerdo a los Anexo I y II de la Directiva del Parlamento Europeo 1999/93/EC y a la ley 59/2003, de 19 de diciembre, de firma electrónica.

La identificación del prestador de servicios de certificación que expide el certificado y el país en el que está establecido (artículo 11.2.c 59/2003)	A través de la información que se recoge en el campo Issuer del certificado tal y como contempla la rfc 3739 En el certificado se recoge claramente el país en el que se establece el PSC en el atributo Country del DN del campo Issuer En la presente DPC y en las Políticas de certificación asociadas, referenciadas en el certificado, se recoge el nombre o razón social, domicilio, dirección electrónica y número de identificación fiscal de la Institución que actúa como PSC la Dirección General de la Policía.
La identificación del firmante (el suscriptor del certificado), por su nombre y apellidos y DNI/NIE o equivalente, o a través de un seudónimo que conste de manera inequívoca. (artículo 11.2.e 59/2003)	A través de la información que se recoge en el campo Subject del certificado tal y como contempla la rfc 3739: Nombre, Apellidos y DNI/NIE. No se contempla la utilización de seudónimos
La inclusión de algún atributo del firmante (el subscriptor), relevante para el uso establecido para el certificado en la Política. (artículo 11.3 59/2003)	Se utilizará la extensión Subject Alternative Name para indicar el cargo, número de carné profesional, dirección de correo y UPN.
Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante. (artículo 11.2.f 59/2003)	La clave pública del suscriptor se encuentra en el certificado tal y como contempla la RFC 5280. (Subject Public Key Info)
El comienzo y el final del periodo de validez del certificado. (artículo 11.2.g 59/2003)	El periodo de validez de las claves y el certificado asociado se encuentra recogido en el campo del certificado contemplado en la ITU-T Recommendation X.509 y en RFC 5280
El código identificativo único del certificado. (artículo 11.2.b 59/2003)	La pareja formada por el Número de serie del certificado y el Issuer tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 5280
La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado. (artículo 11.2.d 59/2003)	La firma digital del emisor del certificado de acuerdo con la ITU-T Recommendation X.509 y la RFC 5280
Los límites de uso del certificado, si se prevén. (artículo 11.2.h 59/2003)	Estos límites estarán reflejados en la Políticas de Certificación asociadas a los certificados y en la extensión KeyUsage tal y como se contempla en la ITU-T Recommendation X.509 y en RFC 5280.
Los límites del valor de las transacciones para las que puede utilizarse el certificado,	No estipulado en el certificado

si se establecen. (artículo 11.2.i 59/2003)

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

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

Requisitos Legales	Modo de cumplimiento
El requisito B) establece la necesidad de un servicio de comprobación del estado de los certificados. (artículo 18.d 59/2003)	La extensión AIA (Authority Information Access) contiene la URL del servicio de validación de certificados.
El requisito i) establece un periodo mínimo de retención de la información relevante (artículo 20.1.f 59/2003)	No estipulado en el certificado No se prevé la destrucción de la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación, aunque de establecer un periodo de retención, este no sería inferior a los 15 años establecidos en la ley de Firma 59/2003
El requisito K) establece que los términos y condiciones de uso de los certificados deben estar accesibles a las terceras partes que hacen uso del certificado. (artículo II.19.2 59/2003)	En la extensión CertificatePolicies se indica la URL en la que están accesibles esta DPC y las Políticas de Certificación asociada

7.1.3 Perfiles de certificados de Sedes electrónicas

Certificado de Sede electrónica Nivel Alto		
CAMPO	**CONTENIDO**	**CRÍTICA**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption)	
4. Issuer Distinguished Name	CN=AC DGP XXX OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	36 meses	
6. Subject	CN= sede.policia.gob.es SERIALNUMBER= S2816015H OU= CUERPO NACIONAL DE POLICIA OU=SEDE ELECTRONICA ADMINISTRATIVA O=MINISTERIO DE INTERIOR C=ES	

Certificado de Sede electrónica Nivel Alto		
CAMPO	**CONTENIDO**	**CRÍTICA**
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	*serverAuth* 1.3.6.1.5.5.7.3.1	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.1.102.34 OID asociado a la PC de certificado de autenticación de funcionario.	
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod:15 Años	NO
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*. Tipo=SEDE ELECTRONICA ADMINISTRATIVA. OID: 2.16.724.1.3.5.1.1.1 - *entidad*. Entidad Suscriptora=AMBITO DEL CUERPO NACIONAL DE LA POLICIA. OID: 2.16.724.1.3.5.1.1.2 - *nif entidad.* NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.1.1.3 - *nombre*. Nombre sede=CUERPO NACIONAL DE POLICIA. OID: 2.16.724.1.3.5.1.1.4 - *dominio*. Nombre Dominio IP=SEDE.POLICIA.GOB.ES. OID: 2.16.724.1.3.5.1.1.5	NO
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	

Certificado de Sede electrónica Nivel Alto		
CAMPO	**CONTENIDO**	**CRÍTICA**
11. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es)CA: URL-AC-R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

Certificado de Sede electrónica Nivel Medio		
CAMPO	**CONTENIDO**	**CRÍTICA**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption)	
4. Issuer Distinguished Name	CN=AC DGP XXX OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	36 meses	
6. Subject	CN=Nombre de la Sede SERIALNUMBER= S2816015H OU=CUERPO NACIONAL DE POLICIA OU=SEDE ELECTRONICA ADMINISTRATIVA O=MINISTERIO DE INTERIOR C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	

Certificado de Sede electrónica Nivel Medio		
CAMPO	**CONTENIDO**	**CRÍTICA**
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	*serverAuth* 1.3.6.1.5.5.7.3.1	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		
Policy Identifier	2.16.724.1.2.1.102.35 OID asociado a la PC de certificado de autenticación de funcionario.	NO
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod:15 Años	NO
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*. Tipo=SEDE ELECTRONICA ADMINISTRATIVA. OID: 2.16.724.1.3.5.1.2.1 - *entidad*. Entidad Suscriptora=AMBITO DEL CUERPO NACIONAL DE LA POLICIA. OID: 2.16.724.1.3.5.1.2.2 - *nif entidad.* NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.1.2.3 - *nombre*. Nombre sede=NOMBRE SEDE. OID: 2.16.724.1.3.5.1.2.4 - *dominio*. Nombre Dominio IP=NOMBRE.SEDE.POLICIA.GOB.ES. OID: 2.16.724.1.3.5.1.2.5	NO
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	
11. Basic Constraints		
Subject Type	Entidad Final	SI
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es) CA: URL-AC-R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

7.1.4 Perfiles de certificados de Sellos electrónicos

Certificado de Sello electrónico Nivel Alto		
CAMPO	**CONTENIDO PROPUESTO**	**CRÍTICA**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption)[8]	
4. Issuer Distinguished Name	CN=AC DGP XXX OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	36 meses	
6. Subject	CN=NOMBRE SERIALNUMBER= S2816015H OU=SELLO ELECTRONICO O=MINISTERIO DE INTERIOR C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	1	
Non Repudiation	1	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	*Client/auth* (1.3.6.1.5.5.7.3.2) *Secure Email (1.3.6.1.5.5.7.3.4)*	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.1.102.36 OID asociado a la PC de certificado de autenticación de funcionario.	

[8] Durante el primer año de emisión se utilizara *sha1withRsaEncryption* para la garantizar la compatibilidad con las aplicaciones y sistemas que actualmente no soportan *sha256withRsaEncryption*.

Certificado de Sello electrónico Nivel Alto		
CAMPO	**CONTENIDO PROPUESTO**	**CRÍTICA**
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod:15 Años	NO
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*. Tipo=SELLO ELECTRONICO. OID: 2.16.724.1.3.5.2.1.1 - *entidad*.Entidad Suscriptora=AMBITO DEL CUERPO NACIONAL DE LA POLICIA. OID: 2.16.724.1.3.5.2.1.2 - *nif entidad*.NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.2.1.3 - *nombre*.Denominación sistema=NOMBRE. OID: 2.16.724.1.3.5.2.1.5	NO
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	
11. Basic Constraints		
Subject Type	Entidad Final	SI
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es) CA: URL-AC-R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

Certificado de Sello electrónico Nivel Medio		
CAMPO	**CONTENIDO PROPUESTO**	**CRÍTICA**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio/Secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad sha256withRsaEncryption)	
4. Issuer Distinguished Name	CN=AC DGP XXX OU=CNP O=DIRECCION GENERAL DE LA POLICIA C=ES	
5. Validez	36 meses	

Certificado de Sello electrónico Nivel Medio		
CAMPO	**CONTENIDO PROPUESTO**	**CRÍTICA**
6. Subject	CN=NOMBRE SERIALNUMBER= S2816015H OU=SELLO ELECTRONICO O=MINISTERIO DE INTERIOR C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	
Extensiones de X509v3		
1. Subject Key Identifier	Función hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO (RFC 5280)
2. Authority Key Identifier	Función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora (AC subordinada). NO SE incluye la identificación del certificado de la AC emisora (en este caso, DN de la AC Raíz, número de serie de la AC Subordinada).	NO (RFC 5280)
3. KeyUsage		SI (RFCs 5280 y 3739)
Digital Signature	1	
Non Repudiation	1	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	*Client/auth* (1.3.6.1.5.5.7.3.2) *Secure Email (1.3.6.1.5.5.7.3.4)*	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.1.102.37 OID asociado a la PC de certificado de autenticación de funcionario.	
URL CPS	URL-DPC (En la actualidad http://www.policia.es/dpc)	
Notice Referente	Certificado sujeto a la Declaración de Prácticas de Certificación de la DGP, donde se establecen limitaciones en la responsabilidad.	
7.Policy Mappings		
qcStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcRetentionPeriod:15 Años	NO

Certificado de Sello electrónico Nivel Medio		
CAMPO	**CONTENIDO PROPUESTO**	**CRÍTICA**
8. Subject Alternate Names	*e-mail (RFC 822) **DirectoryName con:* - *tipo*.Tipo=SELLO ELECTRONICO. OID: 2.16.724.1.3.5.2.2.1 - *entidad*.Entidad Suscriptora=AMBITO DEL CUERPO NACIONAL DE LA POLICIA. OID: 2.16.724.1.3.5.2.2.2 - *nif entidad*.NIF suscriptora=S2816015H. OID: 2.16.724.1.3.5.2.2.3 - *nombre*.Denominación sistema=NOMBRE. OID: 2.16.724.1.3.5.2.2.5	NO
9. Issuer Alternate Names	No se utilizará	
10. Subject Directory Attributes	No utilizado	
11. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
12. Policy Constraints	No utilizado	
13. CRLDistributionPoints	No utilizado	
14. Auth. Information Access	OCSP: URL-OCSP (en la actualidad http://ocsp.policia.es) CA: URL-AC-R (En la actualidad http://www.policia.es/certs/ACRaiz.crt)	NO (RFC 5280)
15.netscapeCertType	No se utilizará	
16. netscapeRevocationURL	No procede	
17. netscapeCAPolicyURL	No procede	
18. netscapeComment	No procede	
19. BiometricInfo	No se utilizará	

7.1.5 Identificadores de objeto (OID) de los algoritmos

Los Identificadores de Objeto (OID) de los algoritmos Criptográficos utilizados en la actualidad son:

SHA-1 with RSA Encryption (1.2 840.113549.1.1.5)

SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

7.1.6 Formatos de nombres

Los certificados emitidos por la Infraestructura de Clave Pública de la DGP contienen el *distinguished name* X.500 del emisor y del titular del certificado en los campos *issuer name* y *subject name* respectivamente.

7.1.7 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 funcionario estará compuesto de los siguientes elementos:

CN, GN, SN, SerialNumber, OU, OU, O, 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= CN=NOMBRE APELLIDO1 APELLIDO2 – DNI/NIE (con letra) [Firmar] [AUTENTICACION] [CIFRADO]

GN = Nombre

SN = APELLIDO1 APELLIDO2 - DNI/NIE (con letra)

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

Los atributos OU (Organizacional Unit) y O (Organization) representan a la Dirección General de la Policía y serán iguales para todos los certificados, tomando los siguientes valores:

OU=AMBITO DEL CUERPO NACIONAL DE POLICIA

OU=EMPLEADO PUBLICO

O=MINISTERIO DE INTERIOR

C=ES

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

El OID de la presente DPC es 2.16.724.1.2.1.102.1 Se le añade una extensión con formato X.Y que recoge la versión.

De esta forma el OID 2.16.724.1.2.1.102.1.X.Y correspondería a la release Y de la versión X de esta DPC

Los identificadores de las Políticas de Certificación asociadas bajo las que se emiten los certificados de la Infraestructura de Clave Pública de la DGP son los siguientes:

Política de Certificados Reconocidos de Firma Electrónica	2.16.724.1.2.1.102.30 (compatible con 0.4.0.1456.1.1)
Política de Certificados Reconocidos de Autenticación	2.16.724.1.2.1.102.31 (compatible con 0.4.0.1456.1.1)
Política de Certificados Reconocidos de Cifrado	2.16.724.1.2.1.102.32 (compatible con 0.4.0.1456.1.1)
Política de Certificados de Sede Electrónica de Nivel ALTO	2.16.724.1.2.1.102.34
Política de Certificados de Sede Electrónica de Nivel MEDIO	2.16.724.1.2.1.102.35
Política de Certificados de Sello Electrónico	2.16.724.1.2.1.102.36

de Nivel ALTO

Política de Certificados de Sello Electrónico de Nivel MEDIO	2.16.724.1.2.1.102.37

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

7.1.9 Uso de la extensión "PolicyConstraints"

No estipulado

7.1.10 Sintaxis y semántica de los "PolicyQualifier"

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

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

7.1.11 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 ACs (con lo que no se limitará para un futuro el conjunto de políticas que se podrán emitir bajo el dominio de certificación de la Infraestructura de Clave Pública de la Dirección General de la Policía). En los certificados de funcionario de autenticación, firma y cifrado se incluirían respectivamente los identificadores de política para firma (2.16.724.1.2.1.102.30), autenticación (2.16.724.1.2.1.102.31) y cifrado (2.16.724.1.2.1.102.32) recogidos en esta DPC. De la misma forma se incluirán los correspondientes Identificadores de política de certificación para los certificados de Sede Electrónica (niveles Medio y Alto) y para los certificados de Sello Electrónico (niveles Medio y Alto).

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

7.2 PERFIL DE ARL Y CRL

La ARL emitida por la AC Raíz será emitida manualmente, en las ocasiones en que sea necesario por revocación de alguna AC Subordinada, tendrá una validez de seis (6) meses y en todo caso se emitirá al menos una vez cada tres (3) meses.

La AC que emite las listas de CRLs emitirá una CRL indirecta completa que contendrá la identificación de todos los certificados revocados no caducados emitidos por la Infraestructura de Clave Pública de la DGP. Es una CRL indirecta, por lo que incluirá la

extensión 2.5.29.29 (*Certificate Issuer*) en cada entrada de revocación con las consideraciones que recoge la RFC 5280 (*"On subsequent entries in an indirect CRL, if this extension is not present, the certificate issuer for the entry is the same as that for the preceding entry"*). La validez de esta CRL estará establecida en 48 horas y será actualizada después de cada revocación o cada 23 horas (garantizándose así la disponibilidad de una nueva CRL antes de que se alcance la fecha indicada en el campo *nextUpdate*).

La ARL y la CRL completa estarán accesibles mediante los siguientes mecanismos:

- LDAP: se publicarán en ldap://ldap.policia.es:

  La ARL/CRL será un nodo de tipo *CRLDistributionPoint* que colgará de un nodo único de tipo *pkiCA* (el correspondiente a la AC Raíz y a la ACRL). La ARL/CRL estará contenida en el atributo binario *certificateRevocationList;binary*.

  La estructura de directorio para las ARL/CRL es la siguiente:

  C=ES,O=DIRECCION GENERAL DE LA POLICIA,OU=CNP

  CN=AC RAIZ DGP (nodo de tipo pkiCA)

  CN=CRL (nodo de tipo CRLDistributionPoint)

  CN=ARC DGP 001 (nodo de tipo *pkica*)

  CN=CRLCompleta (nodos de tipo *CRLDistributionPoint*)

  La URL para descargar la ARL es:

  ldap://ldap.policia.es/CN=CRL,CN=AC%20RAIZ%20DGP,OU=CNP,O=DIRECCION%20GENERAL%20DE%20LA%20POLICIA,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

  La URL para descargar la CRL completa es:

  ldap://ldap.policia.es/CN=CRLCompleta,CN=ARC%20DGP%20001,OU=CNP,O=DIRECCION%20GENERAL%20DE%20LA%20POLICIA,C=ES?authorityRevocationList?base?objectclass=cRLDistributionPoint

- HTTP: se publicarán en http://www.policia.es/crls:

  La ARL se ubicará en un archivo binario con nombre *ARL.crl* (http://www.policia.es/crls/ARL.crl).

  La CRL completa se ubicará en un archivo binario con nombre *CRLCompleta.crl (*http://www.policia.es/crls/CRLCompleta.crl).

7.2.1 Número de versión

La infraestructura de Clave Pública de la Dirección general de la Policía soporta y utiliza CRLs X.509 versión 2 (v2)

7.2.2 ARL, CRL y extensiones

La ARL y las CRLs emitidas por el sistema de la DGP serán conformes con las siguientes normas:

- RFC 5280 (2008-05): Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework

7.3 PERFIL DE OCSP

7.3.1 Perfil del certificado OCSP responder

Las autoridades de validación autorizadas para la validación de los certificados emitidos por la DGP, corresponden a una de las infraestructuras desplegadas por la DGP, más concretamente, a la infraestructura del DNIe.

Los certificados de OCSP responder serán emitidos por una de las AC subordinadas del dominio de certificación disponible en la Dirección General de la Policía y serán conformes con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- IETF RFC 2560 Online Certificate Status Protocol – **OCSP**

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

7.3.2 Número de versión

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

7.3.3 Formatos de nombres

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

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

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

CN, OU, O, C

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

CN= AV DNIE <ID Prestador Validacion>

OU=<Datos Prestador Validación>

OU=DNIE

O=DIRECCION GENERAL DE LA POLICIA

C=ES

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

El identificador de las Políticas de Certificación bajo la que se emiten los certificados de OCSP Responder, utilizados para la verificación del estado de los certificados emitidos por la DGP es el siguiente:

Política de Certificados de OCSP Responder	2.16.724.1.2.2.2.5

El OID corresponde a la jerarquía de OIDs definida para la Dirección General de la Policía.

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

7.3.5 Extensiones y Campos del certificado

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

version

serialNumber

subject

issuer

signingAlgorithms

validityPeriod

extKeyUsage

subjectKeyIdentifier

authorityKeyIdentifier issuerAndSerialPresent

KeyUsage. Calificada como crítica.

BasicConstraint. Calificada como crítica.

CertificatePolicies. Calificada como no crítica.

OCSPNocheck

AIA

A continuación se recogen el perfil del certificado de OCSP Responder .

Certificado de OCSP responder		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	No secuencial	
3. Signature Algorithm	Los correspondiente al parámetro SA (en la actualidad SHA256withRSAEncryption SHA1withRSAEncryption) [9]	
4. Issuer Distinguished Name	CN=AC DNIE XXX [10] OU=DNIE O=DIRECCION GENERAL DE LA POLICIA C=ES	
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: La correspondiente al parámetro TC-AC-S (en la actualidad es de 2048 bits).	
Campos de X509v2		
1. issuerUniqueIdentifier	No se utilizará	
2. subjectUniqueIdentifier	No se utilizará	

[9] Inicialmente sha1 para garantizar la interoperabilidad de los clientes

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

Certificado de OCSP responder		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública del sujeto.	NO
2. Authority Key Identifier	Derivada de utilizar la función de hash asociada al parámetro FCR (SHA-1 en la actualidad) sobre la clave pública de la AC emisora.	NO
3. KeyUsage		SI
Digital Signature	1	
ContentCommitment	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	OCSPSigning	
5. privateKeyUsagePeriod	No se utilizará	
6. Certificate Policies		NO
Policy Identifier	2.16.724.1.2.2.2.5	
URL DPC	URL-DPC (En la actualidad http://www.dnie.es/dpc)	
Notice Reference		
7.Policy Mappings	No se utilizará	
8. Subject Alternate Names	No se utilizará	NO
9. Issuer Alternate Names	No se utilizará	
10. Basic Constraints		SI
Subject Type	Entidad Final	
Path Length Constraint	No se utilizará	
11. Policy Constraints	No se utilizará	
12. CRLDistributionPoints	No se utilizará	NO
13. Auth. Information Access	CA : URL-AC-R (En la actualidad http://www.dnie.es/certs/ACraiz.crt)	NO
14. OCSPNoCheck	Valor NULL como contempla la norma	NO

7.3.6 Formato de las peticiones OCSP

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

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

7.3.7 Formato de las respuestas

El OCSP responder de los servicios de validación de la DGP es capaz, al menos, de generar respuestas de tipo id-pkix-ocsp-basic.

Respecto al estado de los certificados responderá como:

- “Revoked”, para aquellos certificados emitidos por las AC definidas en el servicio de validación de la DGP.
- “Good”, para aquellos certificados emitidos por las AC definidas en el servicio de validación de la DGP 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” contiene el instante de tiempo en el que el OCSP responder genera y firma la respuesta
- “thisUpdate”, indica 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”, indica el instante de tiempo en el que se dispondrá de nueva información de revocación. En el caso de certificados revocados deberá contener el campo “nextUpdate” de la CRL que se ha utilizado, salvo cuando la fecha de “nextUpdate” sea anterior a la fecha local. En el resto de casos no se establecerá el campo nextUpdate, lo que es equivalente según rfc2560 a indicar que se puede disponer de nueva información de revocación en cualquier momento, con lo que es responsabilidad del cliente volver a consultar cuando lo estime oportuno

7.3.8 Fechado de respuestas OCSP

El servicio de servicios de validación utiliza como fuente segura de tiempos la establecida oficialmente en España (en la actualidad la del Real Instituto y Observatorio de la Armada) para habilitar los campos de fecha recogidos en el punto anterior.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

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

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

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

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

8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

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

- Todo equipo o persona designada para realizar una auditoría de seguridad sobre el sistema la infraestructura de Clave Pública de la Dirección General de la Policía 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 de la infraestructura de Clave Pública de la Dirección General de la Policía.
- En general los criterios establecidos en la sección 3.4 de la CWA 14172-2 ("*Guidance on requirements for independent bodies, assessors, and assessment teams*.")

8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

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

8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría determinará la adecuación de la infraestructura de Clave Pública de la Dirección General de la Policía con esta DPC. También determinará los riesgos del incumplimiento de la adecuación con la operativa definida por esos documentos.

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

8.5 ACCIONES A EMPRENDER COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

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

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

8.6 COMUNICACIÓN DE RESULTADOS

El equipo auditor comunicará los resultados de la auditoría a la Autoridad de Aprobación de Políticas de la Dirección General de la Policía (AAP), al Gestor de Seguridad y administradores de la infraestructura de Clave Pública de la Dirección General de la Policía, así como a la Autoridad en la que se detecten incidencias.

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 TARIFAS

9.1.1 Tarifas de emisión de certificado o renovación

No aplican.

9.1.2 Tarifas de acceso a los certificados

No aplica.

9.1.3 Tarifas de acceso a la información de estado o revocación

No aplica.

9.1.4 Tarifas de otros servicios tales como información de políticas

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

9.1.5 Política de reembolso

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

9.2 RESPONSABILIDADES ECONÓMICAS

Subsumido en el apartado 9.8.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

9.3.1 Ámbito de la información confidencial

Toda información que no sea considerada por el sistema de la infraestructura de Clave Pública de la Dirección General de la Policía como pública revestirá el carácter de confidencial. Se declara expresamente como información confidencial:

- 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.

- Las claves privadas asociadas a los Certificados de Sede electrónica y Sello

- Las claves privadas asociadas al Carné Profesional:

  Para garantizar la confidencialidad de las claves privadas, de autenticación y firma, del funcionario, la Autoridad de Registro del Carné Profesional proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro en presencia del funcionario titular y de un funcionario de la Dirección General de la Policía y en un puesto que disponga de un dispositivo criptográfico específico.

  Dichas claves serán entregadas al funcionario grabadas en el procesador de su Carné Profesional basado en tarjeta criptográfica. Así mismo tanto la Autoridad de Registro como de Certificación no tendrán la posibilidad de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir estas claves ni para activarlas.

  La clave de cifrado se generará en el momento de expedición del Carné Profesional y será almacenado de forma segura en el Servicio de Archivo y Recuperación de Claves. Este servicio garantiza la confidencialidad de la clave de cifrado, la cual sólo podrá ser recuperada por el propio funcionario, o por personal autorizado actuando de oficio (ver apartado 4.12)

- Confidencialidad en la prestación de servicios de certificación:

  La Dirección General de la Policía publicará exclusivamente los datos del funcionario 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 funcionario de la existencia de un fichero automatizado de datos de carácter personal creado y bajo la responsabilidad de la Dirección General de la Policía, 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 titular de los datos 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 Dirección General de la Policía tiene el deber de guardar secreto establecida legal o convencionalmente.
- Cualquier otra información clasificada.

9.3.2 Información no confidencial

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

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

9.3.3 Deber de secreto profesional

Los funcionarios al servicio de la Dirección General de la Policía que participen en cualesquiera tareas propias o derivadas de la infraestructura de Clave Pública de la Dirección General de la Policía están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa reguladora que les es aplicable.

Asimismo el personal contratado que participe en cualquier actividad u operación de la infraestructura de Clave Pública de la Dirección General de la Policía estará sujeto al deber de secreto en el marco de las obligaciones contractuales contraídas con la Dirección General de la Policía.

9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

9.4.1 Política de protección de datos de carácter personal

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

9.4.2 Información tratada como privada

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

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

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

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

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

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

La información confidencial de acuerdo con la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 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.

9.4.3 Información no calificada como privada

Es considerada no confidencial la siguiente información:

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

9.4.4 Responsabilidad de la protección de los datos de carácter personal

Esta responsabilidad se regula en el capítulo 10.

9.4.5 Comunicación y consentimiento para usar datos de carácter personal

No aplica.

9.4.6 Revelación en el marco de un proceso judicial

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

9.4.7 Otras circunstancias de publicación de información

Estas posibles circunstancias se regulan en el capítulo 10.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

En los términos establecidos en el Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, la Dirección General de la Policía 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 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 la Infraestructura de Clave Pública de la Dirección General de la Policía se utilizará el OID asignado por ISO-ITU-T.

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

9.6 OBLIGACIONES

9.6.1 Obligaciones de la AC

La Autoridad de Certificación *Subordinada* actuará relacionando una determinada clave pública con su titular a través de la emisión de un certificado de firma reconocido, 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 reconocidos y la provisión del dispositivo de creación de firma.

La AC tiene las siguientes obligaciones:

1º Realizar sus operaciones en conformidad con esta DPC.

2º Publicar esta DPC en el sitio web referido en el apartado *2.1 Repositorio*.

3º Comunicar los cambios de esta DPC de acuerdo con lo establecido en el apartado 9.*12.2 Periodo y mecanismo de Notificación*

4º Cursar en línea la solicitud de un certificado y minimizar el tiempo necesario para expedir dicho certificado.

5º Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.

6º Revocar los certificados en los términos de la sección *4.4 Suspensión y Revocación de Certificados* y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web referidos en el apartado *2.1 Repositorio,* con la frecuencia estipulada en el punto *4.9.7 Frecuencia de emisión de CRLs*

7º En el caso que la AC proceda de oficio a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con esta DPC

8º Actualizar en línea y publicar las bases de datos de certificados en vigor y certificados revocados.

9º Poner a disposición de los funcionarios los certificados correspondientes a la(s) Autoridad(es) de Certificación de la Dirección General de la Policía.

10º Proteger la clave privada de la(s) Autoridad(es) de Certificación de la Dirección General de la Policía.

11º Conservar registrada toda la información y documentación relativa a los certificados emitidos por la Dirección General de la Policía durante un mínimo de quince años.

12º Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte

13º No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados del Carné Profesional, para los certificados de firma y autenticación.

14º Colaborar con los procesos de auditoría.

15º Operar de acuerdo con la legislación aplicable. En concreto con:

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica

La L. O. 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal

16º En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ellas emitidos y al Organismo Ministerial competente (en la actualidad el Ministerio de Industria, Energia y Turismo) tal como se recoge en el epígrafe 5.8.1.

9.6.2 Obligaciones de la AR

Las Oficinas de Expedición de Certificados de la Dirección General de la Policía, 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 los certificados al funcionario. No almacenando ni copiando los datos de creación de firma.

4º Tramitar las peticiones de revocación lo antes posible.

5º Notificación al funcionario de la revocación o suspensión de sus certificados cuando se produzca de oficio por la Dirección General de la Policía, o a petición de la Autoridad competente.

6º Comprobar que toda la información incluida o incorporada por referencia en el certificado es exacta así como el resto de los datos que se graben en el procesador de la tarjeta criptográfica del Carné Profesional

7º Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado 10.

9.6.3 Obligaciones de los titulares de los certificados

Es obligación de los titulares de los certificados emitidos bajo la presente DPC:

1º Suministrar a las Autoridades de Registro información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.

2º Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta DPC que le sean de aplicación, así como las modificaciones que se realicen sobre las mismas.

3º Comunicar a la Dirección General de la Policía, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento de los certificados o sus claves privadas.

4º Proteger sus claves privadas y custodiar los Certificados asociados, tomando las precauciones razonables para evitar su pérdida, revelación, alteración o uso no autorizado.

5º Aceptar las restricciones de uso establecidas en esta DPC a las claves y certificados emitidos por la Dirección General de la Policía.

6º 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 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.

7º No revelar la clave de acceso que permite la utilización de los certificados de la Dirección General de la Policía.

8º Informar inmediatamente a la Dirección General de la Policía acerca de cualquier situación que pueda afectar a la validez del Certificado.

9º Asegurarse de que toda la información contenida en el Certificado es correcta. Notificándolo inmediatamente en caso contrario.

10º No monitorizar, manipular o realizar actos de "ingeniería inversa" sobre la implantación técnica (hardware y software) de los servicios de certificación, sin permiso previo por escrito de la Autoridad de Certificación.

11º Cumplir las obligaciones que se establecen para el suscriptor en este documento y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.6.4 Obligaciones de los terceros aceptantes

A) Es obligación de los terceros que acepten y confíen en los certificados emitidos por la Dirección General de la Policía:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y en esta DPC.
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o ha sido o revocado.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez, revocación e los certificados en que confía.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo, utilizando los medios que la DGP publique en los sitios Web https://sede.policia.gob.es y www.policia.es

B) Los prestadores de servicios deberán verificar la validez de las firmas generadas por los certificados emitidos por la Dirección General de la Policía a través del Servicio de Validación de esta Dirección General.

- En el supuesto que no se realice dicha comprobación, la Dirección General de la Policía 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 (bien de sede, sello, autenticación, firma o cifrado) 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 de 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.
- Cuando se realice una operación que pueda ser considerada ilícita o se de un uso no conforme a lo establecido en esta DPC, no se deberá confiar en la firma emitida por el certificado

D) Para confiar en los Certificados emitidos por la Dirección General de la Policía, el prestador de servicios deberá conocer y aceptar toda restricción a que esté sujeto el citado Certificado.

9.6.5 Obligaciones de otros participantes

No estipulado

9.7 LIMITACIONES DE RESPONSABILIDAD

Subsumido en 9.8.

9.8 RESPONSABILIDADES

9.8.1 Limitaciones de responsabilidades

La Autoridad de Certificación de la Dirección General de la Policía responderá en el caso de incumplimiento de las obligaciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y normativa de desarrollo, y en la presente DPC

9.8.2 Responsabilidades de la Autoridad de Certificación

- La Dirección General de la Policía responderá por los daños y perjuicios que causen al firmante o terceros de buena fe cuando incumpla las obligaciones que impone la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extra-contractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.
- De manera particular, la Dirección General de la Policía como prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.
- La Dirección General de la Policía como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas

en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

- La Dirección General de la Policía no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del funcionario y/o del prestador de servicio.
- La Dirección General de la Policía no será responsable de la utilización incorrecta de los Certificados ni de las claves, ni de cualquier daño indirecto que pueda resultar de la utilización de los Certificados.
- La Dirección General de la Policía 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 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 no será responsable del contenido de aquellos documentos firmados electrónicamente por los funcionarios con el Certificado de firma contenido en el Carné Profesional
- La Dirección General de la Policía no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta DPC y en la Ley.

9.8.3 Responsabilidades de la Autoridad de Registro

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los funcionarios y la validación de sus datos, con las mismas limitaciones que se establecen en el apartado anterior para la Autoridad de Certificación.

9.8.4 Responsabilidades del titular de los certificados

El titular de los certificados 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 titular de los certificados 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 titular del certificado.

El Carné Profesional es un documento personal e intransferible emitido por la Dirección General de la Policía que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y es responsable de la conservación del mismo.

9.8.5 Delimitación de responsabilidades

La Autoridad de Certificación de la Dirección General de la Policía no asume ninguna responsabilidad en caso de pérdida o perjuicio:

RESP.1	De los servicios que prestan, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
RESP.2	Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario
RESP.3	Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL
RESP.3	Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta DPC.
RESP.4	Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la infraestructura de Certificación del la Dirección General de la Policía.
RESP.5	Ocasionados por el mal uso de la información contenida en el certificado.
RESP.6	La Autoridad de Certificación no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se autentiquen mediante un certificado emitido por ella.

9.8.6 Cobertura de seguro u otras garantías para los terceros aceptantes

La Dirección General de la Policía como prestador de servicios de certificación no expedirá certificados a personas u organismos ajenos a la Dirección General de la Policía. Por lo que no asume ningún compromiso ni brinda otra garantía, así como tampoco asume otra responsabilidad ante titulares de certificados o terceros aceptantes, que los expuestos anteriormente en esta DPC.

9.9 LIMITACIONES DE PÉRDIDAS

A excepción de lo establecido por las disposiciones de la presente DPC, la Dirección General de la Policía no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros aceptantes.

9.10 PERIODO DE VALIDEZ

9.10.1 Plazo

Esta DPC entra en vigor desde el momento de su publicación en la Orden General y en el repositorio de la Dirección General de la Policía

Esta DPC estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC Raíz, momento en que obligatoriamente se dictará una nueva versión.

9.10.2 Sustitución y derogación de la DPC

Podrán ser sustituidos los parámetros siguientes sin necesidad de derogar o sustituir la totalidad de la DPC:

- FCR: Función Criptográfica de Resumen
- SA: Algoritmo de Firma (*Signature Algoritm*) utilizado por los certificados
- TC-AC-R: Tamaño en bits de las claves de la AC Raíz
- TC-AC-S: Tamaño en bits de las claves de las AC Subordinadas
- TC-C-SS: Tamaño en bits de las claves de los certificados de Sede electrónica y de Sello
- TC-C-CP: Tamaño en bits de las claves de los certificados del Carné
- TV-C-CP: Tiempo de vigencia máxima en meses de los certificados electrónicos reconocidos incorporados al Carné Profesional
- URL-AC-R: URL de los certificados de la AC RAIZ
- URL-AC-S: URL de los certificados de las AC Subordinadas
- URL-ARL**:** URL de la lista de AC revocadas
- URL-DPC: URL de publicación de la DPC
- URL-OCSP: URL del Servicio de validación en línea del estado de los certificados (en la actualidad http://ocsp.policia.es)

Esta DPC será sustituida por una nueva versión en cualquier otra circunstancia, con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la DPC quede derogada se retirará del repositorio público de la Dirección General de la Policía, si bien se conservará durante un periodo de 15 años.

9.10.3 Efectos de la finalización

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

9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Sin perjuicio de lo establecido en el apartado 4º de esta DPC, sobre requisitos operacionales para el ciclo de vida de los certificados, los titulares del Carné Profesional 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 los sitios web https://sede.policia.gob.es y www.policia.es estarán disponibles otros mecanismos de contacto con la entidad competente.

Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

9.12 PROCEDIMIENTOS DE CAMBIOS EN LAS ESPECIFICACIONES

9.12.1 Procedimiento para los cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre esta DPC es la Autoridad de Aprobación de Políticas (AAP). Los datos de contacto de la AAP se encuentran en el apartado *1.5 Administración de las Políticas* de esta DPC.

9.12.2 Periodo y procedimiento de notificación

En el caso de que la AAP juzgue que los cambios en 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 las direcciones de Internet https://sede.policia.gob.es y http://www.policia.es y a través de la Orden General.

9.12.3 Circunstancias en las que el OID debe ser cambiado

En los casos en que, a juicio de la AAP, los cambios de las especificaciones no afecten a la aceptabilidad de los certificados se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los usuarios de los certificados.

En el caso de que la AAP juzgue que los cambios a la especificación pueden afectar a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos últimos números del Identificador de Objeto (OID) que lo representa. Este tipo de modificaciones se comunicará a los usuarios de los certificados según lo establecido en el punto 9.12.2.

9.13 RECLAMACIONES Y JURISDICCIÓN

Todas reclamaciones entre usuarios y la Infraestructura de Clave Pública de la Dirección General de la Policía deberán ser comunicadas por la parte en disputa a la Autoridad de Aprobación de Políticas (AAP) de la Dirección General de la Policía con el fin de intentar resolverlo entre las mismas partes.

9.14 NORMATIVA APLICABLE

Las operaciones y funcionamiento de la Infraestructura de Clave Pública de la Dirección General de la Policía, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- 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 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.
- ORDEN INT/761/2007, de 20 de marzo, por la que se aprueba el nuevo modelo de carné profesional de los funcionarios del Cuerpo Nacional de Policía y otros documentos identificativos.
- El Reglamento Orgánico y otras normas que afecten al funcionamiento de la Dirección General de la Policía

9.15 CUMPLIMIENTO DE LA NORMATIVA APLICABLE

Es responsabilidad de la Autoridad de Aprobación de Políticas velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

9.16 ESTIPULACIONES DIVERSAS

9.16.1 Cláusula de aceptación completa

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

9.16.2 Independencia

En el caso de que una, o más estipulaciones de esta DPC, sea o llegase a ser inválida, nula, o inexigible legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la DPC careciera ésta de toda eficacia jurídica.

9.16.3 Resolución por la vía judicial

No estipulado

9.17 OTRAS ESTIPULACIONES

No se contemplan.

10. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

10.1 RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS

Corresponde a la Dirección General de la Policía, la gestión, administración, uso y custodia de los archivos y ficheros, automatizados o no, relacionados con el Carné Profesional. A tal efecto, la Orden INT/2190/2006, de 19 de junio, por la que se modifica la Orden INT/1751/2002, de 20 de junio, por la que se regulan los ficheros de la Dirección General de la Policía, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispone la aprobación de la creación del fichero SIGESPOL, cuya finalidad es la gestión de recursos humanos de la Dirección General de la Policía, y su sometimiento al ámbito de dicha ley y al régimen general de la misma, constatando que su titularidad corresponde a la DGP, siéndole igualmente de aplicación el Real Decreto 1720/2007, de 21 de diciembre, relativo a las medidas de seguridad exigibles y que han de ser recogidas en el preceptivo Documento de Seguridad.

Todas las entidades que actúen como prestadores de servicios de certificación tendrán, 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 mismo, deberán adoptar su correspondiente documento de seguridad, tal y como se exige para el encargado del tratamiento, el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Se facilitará al interesado el ejercicio de los derechos de oposición, acceso, rectificación y cancelación de sus datos de carácter personal, en los términos y plazos legales.

10.2 CREACIÓN DEL FICHERO E INSCRIPCIÓN REGISTRAL

Los datos de creación e inscripción del fichero SIGESPOL de la Dirección General de la Policía son:

- Nombre de la disposición: ORDEN INT/1031/2012, DE 27 DE ABRIL, POR LA QUE SE MODIFICA LA ORDEN INT/1202/2011, DE 4 DE MAYO
- Publicación: BOLETÍN OFICIAL DEL ESTADO Nº 118, de 17 de MAYO de 2012
- Nº de inscripción en el Registro General de Protección de Datos: 2022840221

Asimismo, el nombre del fichero, su responsable y el área encargada de atender las peticiones de ejercicio de derechos son:

Nombre del Fichero:	SIGESPOL
Responsable del Fichero:	Ministerio del Interior DGP - Cuerpo Nacional de Policía División de Personal

Servicio de Atención al Público:	SECRETARIA GENERAL DE LA DIVISION DE PERSONAL Av. Pío XII 50 28016-MADRID

10.3 DOCUMENTO DE SEGURIDAD LOPD

10.3.1 Aspectos cubiertos

La presente DPC, tal como se señala en el punto 1.1, se ha hecho de acuerdo a la especificación RFC 3647 *"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"* del Internet Engineering Task Force (IETF) para este tipo de documentos.

No obstante lo expuesto en los apartados 5 "Controles de seguridad física, instalaciones, gestión y operacionales" y 8 "Auditorías de cumplimiento y otros controles" de esta DPC y teniendo en cuenta lo dispuesto en el artículo 19.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que considera la DPC como documento de seguridad, a los efectos previstos en la legislación en materia de protección de datos de carácter personal, resulta obligado añadir el presente apartado con objeto de recoger todos los requisitos contemplados en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados con Datos de Carácter Personal
A tal fin se tratan los siguientes aspectos:

- Estructura básica de datos de carácter personal.
- Nivel de seguridad aplicable.
- Sistemas de Información que soportan el fichero
- Relación de usuarios
- Notificación y Gestión de Incidencias
- Copias de respaldo y recuperación
- Control de Accesos
- Ficheros Temporales
- Gestión de Soportes
- Utilización de datos reales en pruebas

El resto de aspectos que debe recoger un Documento de Seguridad han sido ya incluidos en capítulos anteriores de la presente DPC.

El objeto del Documento de Seguridad es preservar los datos de carácter personal procesados por la Infraestructura de Clave Pública de la Dirección General de la Policía, por lo que afecta a todos aquellos recursos (personas, equipos, comunicaciones, software, procedimientos) implicados en el tratamiento de los datos.

10.3.2 Funciones y obligaciones del personal

Esta DPC, así como futuras versiones de la misma, son conocidas por todas las personas que acceden a los datos de carácter personal gestionados por la Infraestructura de Clave Pública de la Dirección General de la Policía, 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 de la Dirección General de la Policía.

10.3.3 Estructura de datos de carácter personal

En la siguiente tabla se recogen los datos, utilizando las denominaciones utilizadas en el formulario de notificación de ficheros a la Agencia Española de Protección de Datos, de los titulares de certificados:

Datos especialmente protegidos:	AFILIACION SINDICAL;
Otros datos especialmente protegidos:	SALUD;
Datos de infracciones:	INFRACCIONES PENALES; INFRACCIONES ADMINISTRATIVAS;
Datos de carácter identificativo:	D.N.I./N.I.F.; NUM.S.S./ MUTUALIDAD; DIRECCION; FIRMA/HUELLA; NUM. REGISTRO PERSONAL; OTROS DATOS DE CARACTER IDENTIFICATIVO; FIRMA ELECTRONICA; IMAGEN/VOZ; TELEFONO; NOMBRE Y APELLIDOS; ARMAS QUE POSEAN, LICENCIAS, AYUDAS DISTINTIVOS Y CARNÉ PROFESIONALES,
Otros tipos de datos:	DATOS DE CARACTERISTICAS PERSONALES; DATOS ACADEMICOS Y PROFESIONALES; DATOS DE INFORMACION COMERCIAL; DATOS ECONOMICOS FINANCIEROS Y DE SEGUROS; DATOS DE DETALLES DE EMPLEO; DATOS DE CIRCUNSTANCIAS SOCIALES;
Sistema de tratamiento:	Automatizado

En el apartado 7 se recoge la estructura detallada del perfil del certificado.

10.3.4 Nivel de seguridad

Dadas las especiales características de seguridad que ha de tener la PKI de la Dirección General de la Policía, el nivel de seguridad que establece esta DPC y la naturaleza de los datos de carácter personal tratados se implantarán medidas de seguridad de nivel alto.

10.3.5 Sistemas de información

Dentro de la estructura de sistemas de información que constituye la PKI de la Infraestructura de Clave Pública de la Dirección General de la Policía 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.

10.3.6 Relación de usuarios

El Coordinador de Seguridad mantiene una relación de los usuarios con acceso a los datos de carácter personal tratados por la PKI en la que se indica su rol y nivel de acceso. Dicha relación de usuarios tiene carácter confidencial por motivos de seguridad, por lo que será precisa una petición motivada al Coordinador de Seguridad para tener acceso a la misma.

No se incluyen en esa relación los usuarios con acceso a los certificados electrónicos a efectos de hacer uso de los mismos para el envío de información cifrada ni los usuarios con acceso a las CRL.

10.3.7 Notificación y gestión de incidencias

Los procedimientos internos del Departamento de Sistemas de Información asociados a la gestión de problemas aseguran que todas las incidencias se registran y documentan, realizándose un seguimiento de las mismas. Se registra información relativa a: fecha, hora, tipo de incidencia, persona que comunica la misma, persona a quien se asigna la resolución de la incidencia, documentación sobre la causa y sus efectos.

El régimen de auditoría previsto está recogido en el apartado 5.4.

10.3.8 Copias de respaldo y recuperación

Las copias de respaldo se realizan de forma diaria conforme a la normativa en vigor de la Dirección General de la Policía para ordenadores centrales.

Las recuperaciones de datos se hacen con la autorización del responsable del fichero:

a. Incidencias en el sistema informático: Se comunica al responsable informático del sistema, quien deberá obtener la autorización del propietario mediante los procedimientos establecidos al efecto.

b. Incidencias en la infraestructura del sistema informático: Se siguen los procedimientos establecidos en los planes de respaldo del Departamento de Sistemas de Información para cada contingencia.

10.3.9 Control de accesos

Las autorizaciones de acceso a los sistemas de información estarán basadas exclusivamente en el principio de necesidad para el trabajo. Los administradores de usuarios y de elementos se encargarán de validar siempre esta necesidad antes de conceder el acceso a los datos.

Asimismo, todos los elementos que permitan acceder a datos personales estarán catalogados como de uso restringido.

El registro de acceso se hace siempre de acuerdo a lo establecido en el artículo 24 del Reglamento de Medidas de Seguridad y recogido en el Documento de Seguridad del Sistema de la Infraestructura de Clave Pública de la Dirección General de la Policía

10.3.10 Ficheros temporales

El software utilizado para generar un certificado electrónico conforme al estándar X.509v3 genera ficheros temporales, ficheros de registros de auditoría, que son debidamente custodiados ante la necesidad de trazabilidad de la instalación por la actividad de prestador de servicios de certificación en cumplimiento de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

El tratamiento de los ficheros temporales está sometido a lo preceptuado en el artículo 87 del Reglamento de Medidas de Seguridad y recogido en el Documento de Seguridad del Sistema de la Infraestructura de Clave Pública de la DGP.

10.3.11 Gestión de soportes

Los soportes internos están correctamente identificados por su código de barras o incluyen su correspondiente etiqueta identificativa.

Los soportes están ubicados en las salas de ordenadores. El acceso a estas salas está restringido, las autorizaciones permanentes son validadas por el Jefe del Departamento de Sistemas de Información y el acceso provisional solo podrá ser autorizado por el Jefe de Explotación o el Jefe de Operación.

Todos los soportes que deban salir de los locales de la DGP cumplirán los siguientes requisitos:

- La salida estará autorizada por el Administrador de la PKI, manteniéndose a estos efectos por el Departamento de Sistemas de Información un registro en papel de la entrada/salida de soportes
- Estos soportes estarán protegidos mediante técnicas criptográficas, de forma que nadie, salvo las propias aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.
- Las salidas por mantenimiento de soportes se someterá a un proceso de borrado físico o desmagnetización.,

La reutilización de soportes que hubieran contenido datos de carácter personal se someterán a un proceso de borrado físico o similar.

10.3.12 Utilización de datos reales en pruebas

No se utilizarán datos personales reales para la realización de pruebas, salvo que se aseguren los mismos niveles de seguridad que establece la presente DPC.

Los procedimientos de pruebas utilizados en el Departamento de Sistemas de Información aseguran el cumplimiento del nivel de seguridad requerido para la utilización de datos reales en pruebas.

ÚLTIMOS CAMBIOS

LISTA DE ÚLTIMOS CAMBIOS

- **Apartado:**

  Cambio:
  - Cambio
  - Cambio

- **Apartado:**

  Cambio:
  - Cambio
  - Cambio

- **Apartado:**

  Cambio:
  - Cambio
  - Cambio