BANCO DE ESPAÑA
Eurosistema

11.05.2015

OID: 1.3.6.1.4.1.19484.2.2.20

Infraestructura de Clave Pública del Banco de España

Políticas de Certificación para certificados de usuario interno

RESUMEN Este documento recoge las Políticas de Certificación (PC) que rigen los certificados de usuario interno emitidos por la Autoridad de Certificación Corporativa de la Infraestructura de Clave Pública (PKI) del Banco de España.

Hoja de Control

Título	Políticas de Certificación para certificados de usuario interno
Autor	Departamento de Sistemas de Información
Versión	1.1
Fecha	11.05.2015

Registro de Cambios

Versión	**Fecha**	**Motivo del cambio**
1.0	20.10.2014	Primera versión que consolida en un único documento las políticas de certificación de todos los certificados para usuario interno del Banco de España
1.1	11.05.2015	Actualización con motivo de la renovación de las Autoridades de Certificación

ÍNDICE

1 Introducción

1.1 Resumen

Este documento recoge las Políticas de Certificación (PC) que rigen los certificados de usuario interno emitidos por la Autoridad de Certificación Corporativa de la Infraestructura de Clave Pública (en adelante PKI) del Banco de España (desde ahora PKIBDE).

Desde el punto de vista de la norma X.509 v3, una PC es un conjunto de reglas que definen la aplicabilidad o uso de un certificado en una comunidad de usuarios, sistemas o clase particular de aplicaciones que tengan en común una serie de requisitos de seguridad.

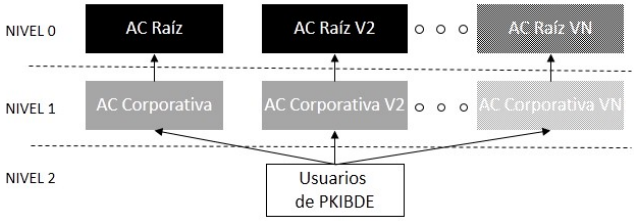
En esta PC se detalla y completa lo estipulado en la "Declaración de Prácticas de Certificación" (DPC) de la PKI del Banco de España (PKIBDE), conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

La presente PC, salvo en el apartado 9 en el que existe una ligera desviación, 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 nuevo capítulo dedicado a la Protección de Datos de Carácter Personal para dar cumplimiento a la legislación española en la materia.

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

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

La arquitectura general, a nivel jerárquico, de la PKI del Banco de España es la siguiente[1]:



[1] Sucesivas renovaciones de las Autoridades de Certificación, sean Raíz o Corporativas, se señalarán con un número de versionado, tal y como se muestra en la imagen.

1.2 Nombre del documento e identificación

Nombre del documento	Políticas de Certificación (PC) para certificados de usuario interno
Versión del documento	1.1
Estado del documento	Aprobado
Fecha de emisión	11.05.2015
OIDs (Object Identifiers)	1.3.6.1.4.1.19484.2.2.20: Políticas de Certificación para certificados de usuario interno (este documento) 1.3.6.1.4.1.19484.2.2.6: Política de Certificación para certificados de autenticación 1.3.6.1.4.1.19484.2.2.12: Política de Certificación para certificados de firma electrónica 1.3.6.1.4.1.19484.2.2.17: Política de Certificación para certificados de cifrado recuperables en software 1.3.6.1.4.1.19484.2.2.8: Política de Certificación para certificados de cifrado (obsoleta) 1.3.6.1.4.1.19484.2.2.15: Política de Certificación para certificados de administrador 1.3.6.1.4.1.19484.2.2.13: Política de Certificación para certificados provisionales de autenticación 1.3.6.1.4.1.19484.2.2.10: Política de Certificación para certificados provisionales de firma electrónica 1.3.6.1.4.1.19484.2.2.16: Política de Certificación para certificados provisionales de administrador
Ubicación de la DPC	http://pki.bde.es/politicas
DPC Relacionada	Declaración de Prácticas de Certificación de la PKI del Banco de España OID 1.3.6.1.4.1.19484.2.2.1

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- El Banco de España como titular de PKIBDE.
- La Autoridad de Administración de Políticas.
- Las Autoridades de Certificación.
- Las Autoridades de Registro.
- Las Autoridades de Validación.
- El Archivo de Claves.
- Los Solicitantes y Titulares de los certificados emitidos por PKIBDE.
- Los Terceros Aceptantes de los certificados emitidos por PKIBDE.

1.3.1 Autoridad de Administración de Políticas

Se define Autoridad de Administración de Políticas de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

1.3.2 Autoridades de Certificación

Se define Autoridades de Certificación de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

Las Autoridades de Certificación que actualmente componen PKIBDE son:

1.3.2.1 Autoridades de Certificación Raíz

- **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= BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Número de serie	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Nombre distintivo del emisor	CN= BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-08 11:34:12 hasta 2034-07-08 11:34:12
Huella digital (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8
Algoritmos criptográficos	SHA-1 / RSA 2048

- **AC Raíz V2**: 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. Se emiten tres certificados válidos, utilizando el mismo par de claves, para esta AC:

    - Con algoritmo SHA-1[2]:

1.3.2.2 Autoridades de Certificación Raíz

- **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=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Número de serie	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-08 11:34:12 hasta 2034-07-08 11:34:12
Huella digital (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8
Algoritmos criptográficos	SHA-1 / RSA 2048

[2] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

- **AC Raíz V2**: 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. Se emiten tres certificados válidos, utilizando el mismo par de claves, para esta AC:

  - Con algoritmo SHA-1[3]:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	25B4 07F6 4A5C F9F1 5547 7951 2040 982B
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	A84A 2C75 2746 B21B 567F 8B07 EC2A FCB9 7551 046A
Algoritmos criptográficos	SHA-1 / RSA 4096

  - Con algoritmo SHA-256:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	4554 22D4 E876 1BFC 5547 4D19 4E85 6E37
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	ACBC CB74 406A 5588 EB88 2F5F 5994 9DDC B831 7986
Algoritmos criptográficos	SHA-256 / RSA 4096

  - Con algoritmo SHA-512:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	19D8 C7AA 668C 3E0F 5547 7970 D573 00FC
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	2AD9 E9BF FCDD B5D4 46C9 7A3A D4BB 6DCE A3B1 219C
Algoritmos criptográficos	SHA-512 / RSA 4096

La AC Raíz V2 ha sido emitida para sustituir a la AC Raíz de Banco de España, con motivo de la actualización criptográfica de los algoritmos y tamaños de clave utilizados de acuerdo a las recomendaciones internacionales. Ambas AC Raíz son válidas, sin embargo, hasta su fecha de caducidad.

[3] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

1.3.2.3 Autoridades de Certificación Intermedias

- **AC Corporativa**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Sus datos más relevantes son:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES
Número de serie	366A 524D A5E4 4AF8 4108 A140 9B9B 76EB
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-29 9:03:28 hasta 2019-07-29 9:03:28
Huella digital (SHA-1)	ABE6 1ED2 5AF6 4253 F77B 322F 6F21 3729 B539 1BDA
Algoritmos criptográficos	SHA-1 / RSA 2048

- **AC Corporativa V2**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Se emiten tres certificados válidos para esta AC:

  - Con algoritmo SHA-1[4]:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	5F8B 48ED 492D 5236 5547 7730 704F 397F
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	4832 0271 9F45 67EB 42E4 4A13 04DE D1F7 7B7B 7EE9
Algoritmos criptográficos	SHA-1 / RSA 4096

  - Con algoritmo SHA-256:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	18D8 765B E681 86C6 5547 76F5 9227 2480
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	A8F0 5CAC 9C65 18C0 8FF6 3F82 C338 DE46 D8B9 3E38
Algoritmos criptográficos	SHA-256 / RSA 4096

  - Con algoritmo SHA-512:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	293F 0A37 5B54 D2D2 5547 7749 5728 B9B6

[4] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

Nombre distintivo del emisor	CN= BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	B3CF 4285 869F 6C07 45B1 D69C 8EC2 7683 6953 DE5E
Algoritmos criptográficos	SHA-512 / RSA 4096

La AC Corporativa V2 ha sido emitida para sustituir a la AC Corporativa de Banco de España, con motivo de la actualización criptográfica de los algoritmos y tamaños de clave utilizados de acuerdo a las recomendaciones internacionales.

Ambas AC Intermedias son válidas hasta su fecha de caducidad o su revocación. Sin embargo, la AC Corporativa dejará de prestar servicio de emisión de certificados de entidad final a partir de la fecha de entrada en servicio de la AC Corporativa V2 manteniéndose únicamente para permitir la revocación de certificados previamente emitidos por ella.

1.3.2.4 Autoridades de Certificación Raíz

- **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=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Número de serie	F16D 7586 5D7C CF92 41AD A17A CD9A 3DE2
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-08 11:34:12 hasta 2034-07-08 11:34:12
Huella digital (SHA-1)	2B60 DE7D 3337 8BF7 5B67 8B10 77BB F951 6029 D6A8
Algoritmos criptográficos	SHA-1 / RSA 2048

- **AC Raíz V2**: 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. Se emiten tres certificados válidos, utilizando el mismo par de claves, para esta AC:

  - Con algoritmo SHA-1[5]:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	25B4 07F6 4A5C F9F1 5547 7951 2040 982B
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	A84A 2C75 2746 B21B 567F 8B07 EC2A FCB9 7551 046A
Algoritmos criptográficos	SHA-1 / RSA 4096

  - Con algoritmo SHA-256:

[5] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	4554 22D4 E876 1BFC 5547 4D19 4E85 6E37
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	ACBC CB74 406A 5588 EB88 2F5F 5994 9DDC B831 7986
Algoritmos criptográficos	SHA-256 / RSA 4096

- Con algoritmo SHA-512:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	19D8 C7AA 668C 3E0F 5547 7970 D573 00FC
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 12:42:33 hasta 2045-05-04 12:42:33
Huella digital (SHA-1)	2AD9 E9BF FCDD B5D4 46C9 7A3A D4BB 6DCE A3B1 219C
Algoritmos criptográficos	SHA-512 / RSA 4096

La AC Raíz V2 ha sido emitida para sustituir a la AC Raíz de Banco de España, con motivo de la actualización criptográfica de los algoritmos y tamaños de clave utilizados de acuerdo a las recomendaciones internacionales. Ambas AC Raíz son válidas, sin embargo, hasta su fecha de caducidad.

1.3.2.5 Autoridades de Certificación Intermedias

- **AC Corporativa**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Sus datos más relevantes son:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES
Número de serie	366A 524D A5E4 4AF8 4108 A140 9B9B 76EB
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2004-07-29 9:03:28 hasta 2019-07-29 9:03:28
Huella digital (SHA-1)	ABE6 1ED2 5AF6 4253 F77B 322F 6F21 3729 B539 1BDA
Algoritmos criptográficos	SHA-1 / RSA 2048

- **AC Corporativa V2**: Autoridad de Certificación subordinada de la AC Raíz. Su función es la emisión de certificados para los usuarios de PKIBDE. Se emiten tres certificados válidos para esta AC:

- Con algoritmo SHA-1[6]:

[6] Este certificado sólo se utilizará en sistemas que no soporten los algoritmos superiores

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	5F8B 48ED 492D 5236 5547 7730 704F 397F
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	4832 0271 9F45 67EB 42E4 4A13 04DE D1F7 7B7B 7EE9
Algoritmos criptográficos	SHA-1 / RSA 4096

- Con algoritmo SHA-256:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	18D8 765B E681 86C6 5547 76F5 9227 2480
Nombre distintivo del emisor	CN=BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	A8F0 5CAC 9C65 18C0 8FF6 3F82 C338 DE46 D8B9 3E38
Algoritmos criptográficos	SHA-256 / RSA 4096

- Con algoritmo SHA-512:

Nombre distintivo	CN=BANCO DE ESPAÑA-AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES
Número de serie	293F 0A37 5B54 D2D2 5547 7749 5728 B9B6
Nombre distintivo del emisor	CN= BANCO DE ESPAÑA-AC RAIZ V2, O=BANCO DE ESPAÑA, C=ES
Periodo de validez	Desde 2015-05-04 18:00:00 hasta 2030-05-04 18:00:00
Huella digital (SHA-1)	B3CF 4285 869F 6C07 45B1 D69C 8EC2 7683 6953 DE5E
Algoritmos criptográficos	SHA-512 / RSA 4096

La AC Corporativa V2 ha sido emitida para sustituir a la AC Corporativa de Banco de España, con motivo de la actualización criptográfica de los algoritmos y tamaños de clave utilizados de acuerdo a las recomendaciones internacionales.

Ambas AC Intermedias son válidas hasta su fecha de caducidad o su revocación. Sin embargo, la AC Corporativa dejará de prestar servicio de emisión de certificados de entidad final a partir de la fecha de entrada en servicio de la AC Corporativa V2 manteniéndose únicamente para permitir la revocación de certificados previamente emitidos por ella.

1.3.3 Autoridades de Registro

Se define Autoridades de Registro de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

La emisión de certificados de autenticación se realiza con la intervención de la AR Corporativa, gestionándose las peticiones de modo remoto.

1.3.4 Autoridad de Validación

Se define Autoridad de Validación de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

1.3.5 Archivo de Claves

El Archivo de Claves permite el archivo y recuperación de las claves privadas de los certificados de cifrado. El Archivo de Claves garantiza la confidencialidad de la clave privada y su recuperación exige, como mínimo, la intervención de dos personas.

En esta PC se regulan los procedimientos de petición y tramitación de recuperación de claves asociadas al certificado de cifrado (obsoleto) o de cifrado recuperable en software, que forma parte del paquete de certificados personales (ver sección 1.3.6).

1.3.6 Titulares de los certificados

Se define Titular de acuerdo con la Declaración de Prácticas de Certificación de PKIBDE.

Los tipos de personas que pueden ser titulares de certificados de usuario interno de la AC Corporativa se restringen a los recogidos en el siguiente cuadro:

Entorno de Certificación	Titulares
AC Corporativa	Usuarios internos de Banco de España, que pueden ser empleados, colaboradores y personal de empresas contratadas con acceso a los sistemas de información del Banco de España

Los titulares de certificados descritos arriba podrán obtener cualquiera de los siguientes paquetes de certificados:

- **Certificados personales**. Es un paquete de certificados almacenado en un mismo dispositivo criptográfico (típicamente una tarjeta criptográfica) destinado al uso general de cualquier usuario interno de Banco de España. Está compuesto por los siguientes certificados:
  - Certificado de autenticación, para la autenticación del titular frente los sistemas de información que acepten este mecanismo.
  - Certificado de firma electrónica, para la firma electrónica de correos electrónicos, ficheros y transacciones informáticas. Este certificado no está disponible para el personal de empresas contratadas.
  - Certificado de cifrado (obsoleto[7]) o bien certificado de cifrado recuperable en software, para el cifrado de correo electrónico, ficheros y transacciones.

- **Certificados de administrador**. Es un certificado almacenado en un dispositivo criptográfico (típicamente una tarjeta criptográfica) que se utiliza para la autenticación del titular con una cuenta de administrador frente los sistemas de información que acepten este mecanismo.

- **Certificados provisionales personales**. Es un paquete de certificados almacenado en un dispositivo criptográfico (típicamente una tarjeta criptográfica) que se utiliza en el caso de olvido del dispositivo criptográfico en el que se encuentran los certificados personales habituales del

[7] Este tipo de certificados ya no es emitido por la AC Corporativa, aunque es posible recuperar del Archivo de Claves el correspondiente par de claves de certificados antiguos

titular. Los certificados provisionales personales tienen un período de vigencia máximo de 7 días, aunque el Administrador de Usuarios podrá elegir un período inferior en el momento de la solicitud. Está compuesto por los siguientes certificados:

- Certificado de autenticación, para la autenticación del titular frente a los sistemas de información que acepten este mecanismo.
- Certificado de firma electrónica, para la firma electrónica de correos electrónicos, ficheros y transacciones informáticas. Este certificado no está disponible para el personal de empresas contratadas.

- **Certificados provisionales de administrador**. Es un certificado almacenado en un dispositivo criptográfico (típicamente una tarjeta criptográfica) que se utiliza en el caso de olvido del dispositivo criptográfico en el que se encuentra el certificado de administrador habitual del titular. Los certificados provisionales de administrador tienen un período de vigencia máximo 7 de días, aunque el Administrador de Usuarios podrá elegir un período inferior en el momento de la solicitud.

1.3.7 Terceros aceptantes

Como Terceros Aceptantes se entienden aquellos que hagan uso de los certificados para identificar a las personas titulares de certificados de autenticación de la AC Corporativa de PKIBDE, para validar las firmas electrónicas realizadas por los titulares y para cifrar datos para ellos.

1.3.8 Otros afectados

Solicitantes: personas físicas que han solicitado la emisión de un certificado a PKIBDE.
Administradores de usuarios: personas que dentro del Banco de España gestionan las peticiones de certificados de usuario interno y verifican su correcta obtención.

1.4 Uso de los certificados

1.4.1 Usos apropiados de los certificados

1 Los certificados de usuario interno emitidos por el Banco de España solamente podrán ser utilizados por sus empleados o personal contratado, tanto en sus relaciones internas como en las externas que sean necesarias para el funcionamiento interno, propio u operativo de la Institución.
2 En el ámbito de lo dispuesto en el párrafo anterior, los certificados de usuario interno emitidos por PKIBDE podrán ser utilizados para actividades con trascendencia económica, con las limitaciones que, en su caso, se establezcan de acuerdo con lo dispuesto en el artículo 7.3 y artículo 11, letras h) e i) de la Ley de Firma Electrónica.
Los certificados regulados por esta PC se utilizarán para la autenticación, firma o cifrado, dependiendo de la correspondiente extensión *KeyUsage* y el atributo OID de la extensión *certificatePolicies*.

1.4.2 Limitaciones y restricciones en el uso de los certificados

Cualquier uso no incluido en el apartado anterior queda excluido.

1.5 Administración de las políticas

1.5.1 Banco de España como titular de PKIBDE

Esta PC es propiedad del Banco de España:

Nombre	Banco de España		
Dirección e-mail	pkibde@bde.es		
Dirección	C/Alcalá, 48. 28014 - Madrid (España)		
Teléfono	+34913385000	**Fax**	+34915310059

1.5.2 Persona de contacto

Esta PC está administrada por la Autoridad de Administración de Políticas (AAP) de la PKI del Banco de España:

Nombre	Departamento de Sistemas de Información Autoridad de Administración de Políticas de la PKI del Banco de España		
Dirección e-mail	pkibde@bde.es		
Dirección	C/Alcalá, 522. 28027 - Madrid (España)		
Teléfono	+34913386666	**Fax**	+34913386875

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

Según lo especificado en la DPC de PKIBDE.

1.5.4 Procedimiento de Aprobación de esta PC

Según lo especificado en la DPC de PKIBDE.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

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

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

Certificado electrónico: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma (clave pública) 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.

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 y, si procede, por el Archivo de Claves.

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

Componente informático (o componente): cualquier dispositivo software o hardware susceptible de utilizar certificados electrónicos para su propio uso, con el objeto de identificarse o intercambiar datos firmados o cifrados con terceros aceptantes.

Directorio: repositorio de información al que se accede a través del protocolo LDAP.
Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificados de PKIBDE.
Identificador de usuario: conjunto de caracteres que se utilizan para la identificación unívoca de un usuario en un sistema.
Infraestructura de Clave Pública: es el conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, cifrado, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados electrónicos.
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 PKIBDE, la jerarquía tiene dos niveles, la AC Raíz en el nivel superior garantiza la confianza de sus AC subordinadas.
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 física que solicita un certificado para sí mismo o para un componente informático.
Tercero Aceptante: persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por PKIBDE.
Titular: persona o componente informático para el que se expide un certificado electrónico y es aceptado por éste o por su responsable en el caso de los certificados de componente.

1.6.2 Acrónimos

AAP: Autoridad de Administración de Políticas
AC: Autoridad de Certificación
AR: Autoridad de Registro
AV: Autoridad de Validación
CRL: Certificate Revocation List (Lista de Revocación de Certificados)
C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500
CDP: CRL Distribution Point (Punto de Distribución de CRLs)
CEN: Comité Européen de Normalisation
CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500
CSR: Certificate Signing Request (petición de certificado). Conjunto de datos, que contienen una clave pública y su firma electrónica utilizando la clave privada asociada, enviado a la Autoridad de Certificación para la emisión de un certificado electrónico que contenga dicha clave pública
CWA: CEN Workshop Agreement
DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500
DPC: Declaración de Prácticas de Certificación
ETSI: European Telecommunications Standard Institute
FIPS: Federal Information Processing Standard (Estándar USA de procesado de información)
HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro
IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)
LDAP: Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio)

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

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

OID: Object identifier (Identificador de objeto único)

OU: 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 (número de identificación personal). Contraseña que protege el acceso a una tarjeta criptográfica.

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

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

PKIBDE: PKI del Banco de España

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

PSC: Prestador de Servicios de Certificación.

PUK: PIN UnlocK Code (código o clave de desbloqueo del PIN). Contraseña que permite desbloquear una tarjeta criptográfica que ha sido bloqueada por introducción consecutiva de un PIN incorrecto.

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

2 Repositorios y publicación de información

2.1 Repositorios

Según lo especificado en la DPC de PKIBDE.

2.2 Publicación de información de certificación

Según lo especificado en la DPC de PKIBDE.

2.3 Temporalidad o frecuencia de publicación

Según lo especificado en la DPC de PKIBDE.

2.4 Controles de acceso a los repositorios

Según lo especificado en la DPC de PKIBDE.

3 Identificación y autenticación de los titulares de los certificados

3.1 Nombres

3.1.1 Tipos de nombres

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

El atributo CN (Common Name) del DN comienza por un prefijo que identifica el uso del certificado, correspondiéndose con uno de los siguientes valores:

Certificados personales

- [A] Certificado de autenticación
- [F] Certificado de firma electrónica
- [C] Certificado de cifrado (obsoleto) y certificado de cifrado recuperable en software

Certificados de administrador

- [X] Certificado de administrador

Certificados provisionales personales

- [A] Certificado provisional de autenticación
- [F] Certificado provisional de firma electrónica

Certificados provisionales de administrador

- [X] Certificado provisional de administrador

El prefijo está seguido del nombre y los dos apellidos del titular del certificado.

Adicionalmente se utilizan los siguientes campos:

- SerialNumber= <Doc. Identificación> (OID: 2.5.4.5)
- PS= <Código Usuario> (OID: 2.5.4.65)

El resto de atributos del DN tendrá los siguientes valores fijos:

- Para el caso de empleados y colaboradores del Banco de España:
  OU=PERSONAS, O=BANCO DE ESPAÑA, C=ES
- Para el caso de personal de empresas contratadas:
  OU=PERSONAS, OU=EMPRESAS EXTERNAS, O=BANCO DE ESPAÑA, C=ES

3.1.2 Necesidad de que los nombres sean significativos

En todos los casos los nombres distintivos de los certificados han de ser significativos y se aplicarán las reglas establecidas en el apartado anterior para ello.

3.1.3 Reglas para interpretar varios formatos de nombres

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

3.1.4 Unicidad de los nombres

El DN de los certificados no puede estar repetido. La utilización del código único de usuario garantiza la unicidad del DN.

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 este documento.

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

Dependiendo del tipo de certificado, el medio de prueba de posesión de la clave privada será diferente:

Certificados personales

- [A] Certificado de autenticación: el par de claves del certificado es generado por el titular en un dispositivo criptográfico y proporcionado a la AC Corporativa la clave pública para su certificación.
- [F] Certificado de firma electrónica: el par de claves del certificado es generado por el titular en un dispositivo criptográfico y proporcionado a la AC Corporativa la clave pública para su certificación.
- [C] Certificado de cifrado (obsoleto) y certificado de cifrado recuperable en software: el par de claves del certificado es generado por la AC Corporativa, por lo que esta sección no es de aplicación para este certificado.

Certificados de administrador

- [X] Certificado de administrador: el par de claves del certificado es generado por el titular en un dispositivo criptográfico y proporcionado a la AC Corporativa la clave pública para su certificación.

Certificados provisionales personales

- [A] Certificado provisional de autenticación: el par de claves del certificado es generado por el titular en un dispositivo criptográfico y proporcionado a la AC Corporativa la clave pública para su certificación.
- [F] Certificado provisional de firma electrónica: el par de claves del certificado es generado por el titular en un dispositivo criptográfico y proporcionado a la AC Corporativa la clave pública para su certificación.

Certificados provisionales de administrador

- [X] Certificado provisional de administrador: el par de claves del certificado es generado por el titular en un dispositivo criptográfico y proporcionado a la AC Corporativa la clave pública para su certificación.

3.2.2 Autenticación de la identidad de una persona jurídica

No está contemplada la emisión de certificados para personas jurídicas.

3.2.3 Autenticación de la identidad de una persona física

La autenticación de la identidad de una persona física es presencial. El solicitante se ha de presentar ante su Administrador de usuarios debidamente identificado mediante su tarjeta de identificación o de otro documento de identificación válido en derecho.

3.2.4 Información no verificada sobre el solicitante

Toda la información recabada en el apartado anterior ha de ser verificada.

3.2.5 Comprobación de las facultades de representación

No estipulado al no estar contemplada la emisión de certificados para personas jurídicas.

3.2.6 Criterios para operar con AC externas

Según lo especificado en la DPC de PKIBDE.

3.3 Identificación y autenticación en las peticiones de renovación de claves

3.3.1 Identificación y autenticación por una renovación de claves de rutina

El proceso de identificación individual será presencial y con los mismos criterios que en la solicitud inicial.

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

El proceso de identificación individual será presencial y con los mismos criterios que en una renovación de rutina.

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 usuario interno emitidos por la AC Corporativa. Aunque estos certificados se van a almacenar en dispositivos criptográficos (típicamente una tarjeta criptográfica), no es objeto de esta Política de Certificación regular la gestión de dichas tarjetas, por lo que siempre se parte de que el solicitante del certificado ha obtenido previamente su dispositivo criptográfico.
Por otro lado, en este capítulo se van a emplear algunas ilustraciones para facilitar su comprensión. En el caso de que existiera alguna diferencia o discrepancia entre lo recogido en el texto y lo recogido en las ilustraciones prevalecerá siempre el texto, dado el carácter necesariamente sintético de las ilustraciones.

4.1 Solicitud de certificados

4.1.1 Quién puede efectuar una solicitud

La petición de los certificados de usuario interno está permitida para los siguientes colectivos:

- Empleados: se entiende que la petición se efectúa automáticamente por el hecho de su incorporación a la plantilla del Banco de España. El empleado debe acudir al Administrador de Usuarios que tenga asignado con su tarjeta de identificación para que éste le identifique, le registre previamente en la PKI y active la emisión de los certificados.
- Colaboradores y subcontratados: la petición la debe hacer el Departamento en el que estén asignados en función de su necesidad de acceder a los sistemas de información. El colaborador o subcontratado deberá ir al Administrador de Usuarios que tenga asignado con su tarjeta de identificación u otro documento de identificación válido en derecho para que dicho Administrador le identifique, le registre previamente en la PKI y active la emisión de los certificados.

La solicitud del certificado no implica su obtención si el solicitante no cumple los requisitos establecidos en la DPC y en esta PC. El Administrador de la PKI podrá recabar del solicitante la documentación que considere oportuna.

4.1.2 Registro de las solicitudes de certificados y responsabilidades de los solicitantes

Este proceso se basa en los siguientes pasos:

1 El solicitante, una vez que dispone de su dispositivo criptográfico (típicamente una tarjeta criptográfica), se dirige al Administrador de Usuarios que tiene asignado.

2 El Administrador de Usuarios comprueba que el solicitante dispone de un dispositivo criptográfico válido y, si el dispositivo es nuevo, comprueba que el solicitante cambia los valores de PIN y PUK de fábrica.

3 El Administrador de Usuarios identifica al solicitante y, utilizando la aplicación de gestión de certificados, introduce los datos del solicitante, selecciona el tipo de certificados requerido, y activa la solicitud de certificados. La Autoridad de Registro realiza el alta de dicha solicitud y la mantiene en estado latente.

4 El solicitante accede a la Autoridad de Registro, obtiene el formulario de Aceptación de las Condiciones de uso de certificados de uso interno, y lo firma de forma manuscrita para así adquirir la condición de titular de los certificados.

5 La Autoridad de Registro genera una contraseña de un solo uso necesaria para poder obtener el paquete de certificados. La contraseña es fragmentada en dos partes, una de las cuales es enviada al solicitante (contraseña de usuario) y la otra al Administrador de Usuarios (contraseña de administrador).

6 El solicitante entrega al Administrador de Usuarios el formulario de Aceptación de Condiciones, quien también lo firma y recoge para su archivo, y entrega al solicitante la contraseña de administrador.

7 El solicitante, utilizando las contraseñas de usuario y de administrador, activa el proceso de generación de los certificados en la Autoridad de Registro.

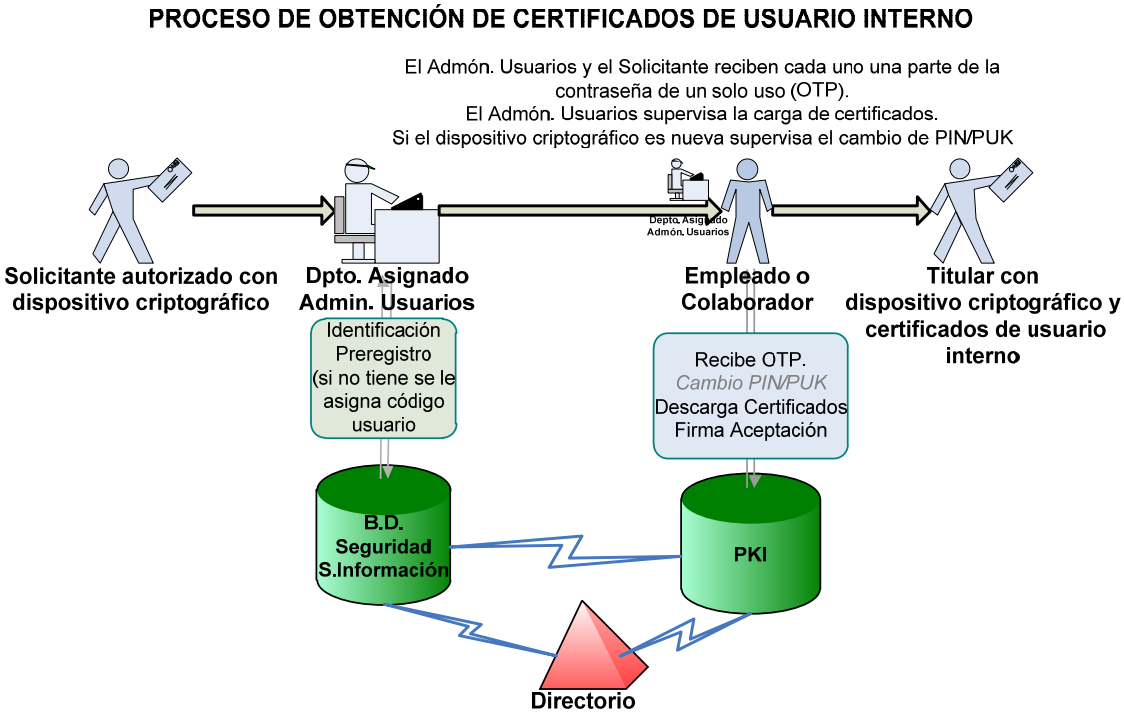
8 La Autoridad de Registro interactúa con el dispositivo criptográfico, para lo cual es necesaria la introducción del PIN por parte del solicitante, y sobre dicho dispositivo se generan los pares de claves requeridos (ver apartado 3.2.1)

9 La Autoridad de Registro envía las claves públicas a la AC Corporativa, la cual emite los certificados y también genera el par de claves de cifrado (ver apartado 3.2.1)

10 La Autoridad de Registro inserta en el dispositivo criptográfico del solicitante los certificados y el par de claves de cifrado emitidos por la AC Corporativa.

Las responsabilidades de los solicitantes no recogidas en este apartado se incluyen en la DPC de PKIBDE.

En la siguiente figura se sintetiza el proceso de obtención de los certificados de usuario interno:



Además del proceso descrito, un Administrador remoto de la AC puede introducir directamente una solicitud de los certificados, descargándolos en el dispositivo criptográfico del solicitante.

4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

La identificación y autenticación del solicitante la realiza el Administrador de Usuarios en todos los casos: emisión inicial, renovación por pérdida o cambio del dispositivo criptográfico y renovación por caducidad.

4.2.2 Aprobación o denegación de las solicitudes de certificados

La emisión del certificado tendrá lugar una vez que PKIBDE haya llevado a cabo las verificaciones necesarias para validar la solicitud de certificación.

La AC Corporativa puede negarse a emitir un certificado de cualquier solicitante basándose exclusivamente en su propio criterio, sin que ello implique contraer responsabilidad alguna por las consecuencias que puedan derivarse de tal negativa.

Las solicitudes de certificados de los empleados del Banco de España se aprueban por su condición de tales, mientras que la de los colaboradores y subcontratados requieren, para ser aprobadas, la previa petición de los certificados por parte del Departamento en el que estén asignados.

4.2.3 Plazo para la tramitación de las solicitudes de certificados

La AC Corporativa de PKIBDE no se hace responsable de las demoras que puedan surgir en el periodo comprendido entre la solicitud de los certificados, su publicación en el repositorio de PKIBDE y la entrega del mismo. En la medida de lo posible la AC Corporativa tramitará las peticiones en menos de 24 horas.

El solicitante dispone de un periodo limitado de 30 días naturales para activar la generación y descarga de los certificados. Pasado ese periodo la petición queda anulada.

4.3 Emisión de certificados

4.3.1 Actuaciones de la AC durante la emisión certificados

La emisión de los certificados implica la autorización definitiva de la solicitud por parte de la AC.

Cuando la AC Corporativa de PKIBDE emita certificados 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 a los 15 días naturales 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 de los certificados.

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

El solicitante conocerá la disponibilidad de los certificados mediante correo electrónico.

4.4 Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

El solicitante deberá confirmar la aceptación de los certificados de usuario interno y sus condiciones mediante firma manuscrita.

4.4.2 Publicación del certificado por la AC

Los certificados de uso interno se publicarán en el repositorio de PKIBDE.

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

No procede.

4.5 Par de claves y uso del certificado

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

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado.
Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC y sólo para lo que éstas establezcan.
Tras la expiración o revocación del certificado el titular dejará de usar la clave privada.
Los certificados regulados por esta PC sólo pueden ser utilizados para prestar los siguientes servicios de seguridad:

Certificados personales

- Certificado de autenticación: autenticación del titular frente a los sistemas de información que admitan este mecanismo.
- Certificado de firma electrónica: firma electrónica de correos electrónicos, ficheros y transacciones informáticas a los que se quiera dotar de control de identidad del firmante, control de integridad y no repudio.
- Certificados de cifrado (obsoleto) y de cifrado recuperable en software: cifrado de correo electrónico, ficheros y transacciones.

Certificados de administrador: autenticación del titular con una cuenta de administrador frente a los sistemas de información que admitan este mecanismo y firma electrónica por parte del titular.

Certificados provisionales personales

- Certificado provisional de autenticación: autenticación del titular frente a los sistemas de información que admitan este mecanismo.
- Certificado provisional de firma electrónica: firma electrónica de correos electrónicos, ficheros y transacciones informáticas a los que se quiera dotar de control de identidad del firmante, control de integridad y no repudio.

Certificados provisionales de administrador: autenticación del titular con una cuenta de administrador frente a los sistemas de información del Banco de España que demanden la comprobación de la identidad del titular mediante certificado electrónico y firma electrónica por parte del titular.

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 PC 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 la DPC y en esta PC. 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

Todas las renovaciones de certificados realizadas en el ámbito de esta PC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de los puntos del apartado 4.6 (4.6.2 a 4.6.7) que establece la RFC 3647, lo que implica, a efectos de esta PC, su no estipulación.

4.7 Renovación de certificados con cambio de claves

4.7.1 Circunstancias para una renovación con cambio claves de un certificado

Los certificados de usuario interno pueden ser renovados, entre otros, por los siguientes motivos:

- Expiración del periodo de validez.
- Cambio de datos contenidos en los certificados.
- Claves comprometidas o pérdida de fiabilidad de las mismas.
- Cambio de formato.

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

4.7.2 Quién puede pedir la renovación de un certificado

La renovación la debe solicitar el titular del certificado.

4.7.3 Tramitación de las peticiones de renovación de certificados con cambio de claves

Este apartado no es de aplicación para los certificados provisionales (tanto personales como de administrador) ya que estos no se renuevan. Si se requieren certificados provisionales antes de que hayan caducado los anteriores, se podrán solicitar de nuevo.

La AC comprobará en el proceso de renovación que la información utilizada para verificar la identidad y atributos del titular es todavía válida. Si alguna información del titular ha cambiado ésta deberá ser verificada y registrada con el acuerdo del titular.

La identificación y autenticación para la renovación de certificados de usuario interno se realizará de forma presencial en los puestos de registro, de forma análoga al caso de la emisión inicial.

Si alguna de las condiciones establecidas en esta PC han cambiado se deberá asegurar que tal hecho es conocido por el titular de los certificados y que éste está de acuerdo con las mismas.

En cualquier caso la renovación de los certificados está supeditada a:

- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que PKIBDE establece a tal efecto. Sólo se puede solicitar la renovación de los certificados dentro de sus últimos 90 días de vigencia.
- Que la AC no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación / suspensión del certificado.
- Que la solicitud de renovación de servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

4.7.4 Notificación de la emisión de un nuevo certificado al titular

Se notificará mediante correo electrónico.

4.7.5 Forma de aceptación del certificado con las claves cambiadas

El titular confirma la aceptación de los certificados mediante la firma del formulario de aceptación de condiciones.

4.7.6 Publicación del certificado con las nuevas claves por la AC

Los certificados de uso interno se publicarán en el repositorio de PKIBDE.

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 Circunstancias para la modificación de un certificado

Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán como una renovación de certificados, por lo que son de aplicación los apartados anteriores al respecto.

En consecuencia, no se recogen el resto de subapartados del apartado 4.8 (4.8.2 a 4.8.7) que establece la RFC 3647, lo que implica a efectos de esta PC que no han sido regulados.

4.9 Revocación y suspensión de certificados

4.9.1 Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su caducidad. El efecto de la revocación de un certificado es la pérdida de vigencia del mismo, 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 revocación de un certificado impide el uso legítimo del mismo por parte del titular.

La revocación de un certificado implica su publicación en la Lista de Revocación de Certificados (CRL) de acceso público.

Los certificados de usuario interno pueden ser revocados por:

- El robo, pérdida, revelación, modificación, u otro compromiso o sospecha de compromiso de la clave privada del titular.
- El mal uso deliberado de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales contenidos en el Formulario de aceptación de las condiciones de los servicios de certificación de la autoridad de certificación del Banco de España, en la DPC o en la presente PC.
- El titular de un certificado deja de pertenecer al grupo, circunstancia que le facultaba para la posesión del certificado.
- Cese de la actividad de PKIBDE.
- Emisión defectuosa de un certificado debido a que:
    1. No se ha cumplido un requisito material para la emisión del certificado.
    2. La creencia razonable de que un dato fundamental relativo al certificado es o puede ser falso.
    3. Existencia de un error de entrada de datos u otro error de proceso.
- El par de claves generado por un titular se revela como “débil”.
- La información contenida en un certificado o utilizada para realizar su solicitud deviene en inexacta.
- Por orden formulada por el titular o por tercero autorizado.
- El certificado de una AR o AC superior en la jerarquía de confianza del certificado es revocado.
- Por la concurrencia de cualquier otra causa especificada en la presente PC o en la DPC.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez del mismo, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta PC ni tendrá efectos retroactivos.

Adicionalmente, los certificados de usuario interno revocados serán eliminados del directorio en el que estaban publicados.

4.9.2 Quien puede solicitar la revocación

PKIBDE o cualquiera de las Autoridades que la componen pueden 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 recomendara emprender dicha acción.

Asimismo, los titulares de certificados también podrán solicitar la revocación de sus certificados, debiendo hacerlo de acuerdo con las condiciones especificadas en el apartado 4.9.3.

La política de identificación para las solicitudes de revocación será la misma que para el registro inicial.

4.9.3 Procedimiento de solicitud de revocación

El titular o persona que solicite la revocación la debe presentar ante su Administrador de Usuarios, identificándose e indicando la causa de la solicitud.

El Administrador de Usuarios tramitará siempre las solicitudes de revocación de aquellos titulares que tenga asignados. La solicitud se realiza mediante una opción dentro de la Aplicación de Administración de Seguridad Informática, asociada a la obtención de nuevos certificados por pérdida del dispositivo criptográfico (típicamente tarjeta criptográfica)

Además de este procedimiento ordinario, los Operadores y Administradores de la PKI podrán revocar de modo inmediato cualquier certificado caso de que llegue a su conocimiento la existencia de alguna causa que motive la revocación.

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 certificados de usuario interno será procesada inmediatamente.

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes

La verificación de las revocaciones es obligatoria para cada uso de los certificados de usuario interno.

Los Terceros Aceptantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargar la nueva CRL del repositorio de PKIBDE al finalizar el periodo de validez de la que posean. Las listas de CRLs guardadas en memoria 'cache'[8], aun no estando caducadas, no garantizan que dispongan de información de revocación actualizada.

Para los certificados de usuario interno el procedimiento ordinario de comprobación de la validez de un certificado será la consulta a la Autoridad de Validación del Banco de España, la cual mediante protocolo OCSP indicará el estado del certificado.

4.9.7 Frecuencia de emisión de CRLs

Según lo especificado en la DPC de PKIBDE.

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

El tiempo máximo admisible entre la generación de la CRL y su publicación en el repositorio es de 1 hora.

[8] Memoria 'caché': memoria donde se guardan los datos necesarios para que el sistema opere con más rapidez en lugar de obtenerlos en cada operación de la fuente de datos. Su uso puede suponer un riesgo de operar con datos no actuales.

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

PKIBDE proporciona un servidor web donde publica las CRLs para la verificación del estado de los certificados que emite. Asimismo, existe una Autoridad de Validación que, mediante el protocolo OCSP, permite verificar el estado de los certificados.

Las direcciones de acceso vía web a las CRL y 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 Autoridad 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 revocación 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 Causas para la suspensión

Los certificados personales de autenticación no serán suspendidos.

4.9.14 Quién puede solicitar la suspensión

No procede.

4.9.15 Procedimiento para la solicitud de suspensión

No procede.

4.9.16 Límites del periodo de suspensión

No procede.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

Según lo especificado en la DPC de PKIBDE.

4.10.2 Disponibilidad del servicio

Según lo especificado en la DPC de PKIBDE.

4.10.3 Características adicionales

Según lo especificado en la DPC de PKIBDE.

4.11 Extinción de la validez de un certificado

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

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

Si no se solicita la renovación del certificado la extinción de su validez supondrá la extinción de la relación entre el titular y la AC.

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de custodia y recuperación de claves

Las únicas claves privadas que se archivan en el Archivo de Clave son las correspondientes a los certificados de cifrado (obsoletos) y de cifrado recuperables en software, que forman parte del paquete de certificados personales.

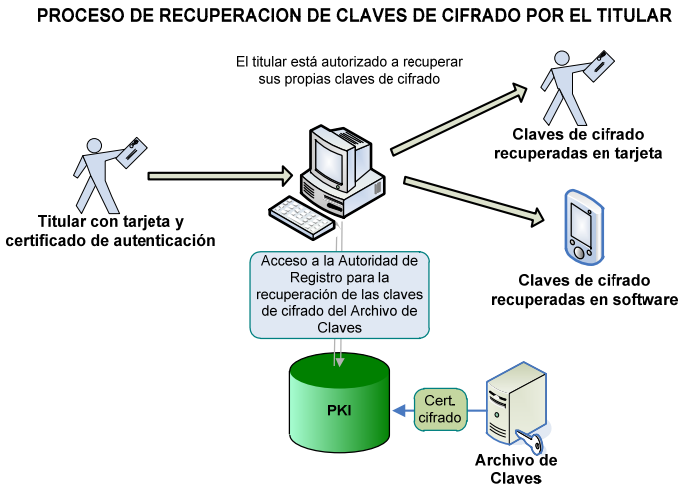
En la recuperación de claves de cifrado se han de distinguir dos casos, dependiendo de si el solicitante es el titular o un tercero. En el caso de que el solicitante sea un tercero, hace falta el concurso de dos figuras separadas, como se describe más adelante, de forma que nadie de forma autónoma pueda acceder a la clave de cifrado de un tercero.

El solicitante es el titular

Se considera que el titular está autorizado a recuperar sus propias claves. Para ello, el titular ha de identificarse con un dispositivo criptográfico con el certificado de autenticación o provisional de autenticación, y acceder a la Autoridad de Registro.

En la Autoridad de Registro podrá recuperar una copia de las claves de cifrado[9], con las siguientes limitaciones:

- Si las claves de cifrado se corresponden a un certificado de cifrado (obsoleto), sólo podrán recuperarse en un dispositivo criptográfico que cumpla las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.
- Si las claves de cifrado se corresponden a un certificado de cifrado recuperable en software, el usuario podrá recuperarlas en un dispositivo criptográfico o bien en formato software según con la especificación PKCS#12, típicamente para su instalación en un dispositivo móvil.



[9] Por razones operativas, PKIBDE podría limitar el número de claves de cifrado que el propio titular puede recuperar a través de la Autoridad de Registro. En este caso, si el titular requiere recuperar claves no disponibles a través de la Autoridad de Registro, podrá solicitar una recuperación basada en los Administradores del Archivo de Claves, tal como se describe más adelante

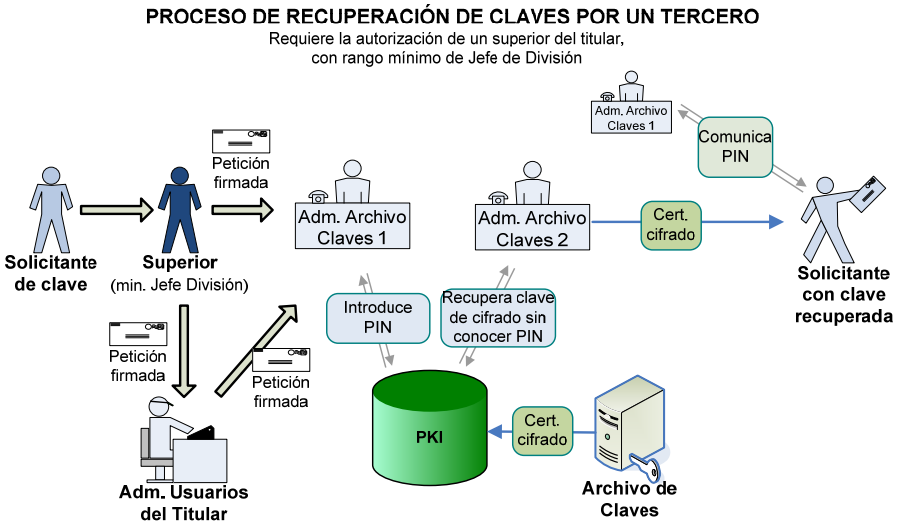
El solicitante es otra persona diferente del titular

La petición de la solicitud de recuperación ha de autorizarla el superior jerárquico del titular con nivel profesional de Jefe de División o equivalente, como mínimo, y el Administrador de Usuarios del titular. En el caso de la Alta Dirección se establecerá un procedimiento especial. El superior ha de remitir su petición firmada al Administrador de Usuarios y a los Administradores del Archivo de Claves. El Administrador de Usuarios, por su parte, ha de confirmar la petición también a los Administradores del Archivo de Claves mediante correo firmado. Una vez cursada la petición, dos Administradores del Archivo de Claves actuarán de la siguiente forma:

1 Tras validar la petición firmada, el primero de los Administradores del Archivo de Claves, en presencia del segundo, accede a la Autoridad de Registro para recuperar del Archivo de Claves un fichero PKCS#12 con las claves privadas de cifrado. La introducción del PIN para proteger el fichero la realizará el segundo Administrador del Archivo de Claves.

2 El primer Administrador del Archivo de Claves facilita el PIN al solicitante

3 El segundo Administrador del Archivo de Claves facilita el fichero PKCS#12 recuperado al solicitante y supervisa la obtención de la clave privada



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

5.1.1 Ubicación física y construcción

Según lo especificado en la DPC de PKIBDE.

5.1.2 Acceso físico

Según lo especificado en la DPC de PKIBDE.

5.1.3 Alimentación eléctrica y aire acondicionado

Según lo especificado en la DPC de PKIBDE.

5.1.4 Exposición al agua

Según lo especificado en la DPC de PKIBDE.

5.1.5 Protección y prevención de incendios

Según lo especificado en la DPC de PKIBDE.

5.1.6 Sistema de almacenamiento

Según lo especificado en la DPC de PKIBDE.

5.1.7 Eliminación de residuos

Según lo especificado en la DPC de PKIBDE.

5.1.8 Copias de seguridad fuera de las instalaciones

No aplicable.

5.2 Controles de procedimiento

5.2.1 Roles responsables del control y gestión de la PKI

Según lo especificado en la DPC de PKIBDE.

5.2.2 Número de personas requeridas por tarea

Según lo especificado en la DPC de PKIBDE.

5.2.3 Identificación y autenticación para cada usuario

Según lo especificado en la DPC de PKIBDE.

5.2.4 Roles que requieren segregación de funciones

Según lo especificado en la DPC de PKIBDE.

5.3 Controles de personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Según lo especificado en la DPC de PKIBDE.

5.3.2 Procedimientos de comprobación de antecedentes

Según lo especificado en la DPC de PKIBDE.

5.3.3 Requerimientos de formación

Según lo especificado en la DPC de PKIBDE.

5.3.4 Requerimientos y frecuencia de actualización de la formación

Según lo especificado en la DPC de PKIBDE.

5.3.5 Frecuencia y secuencia de rotación de tareas

Según lo especificado en la DPC de PKIBDE.

5.3.6 Sanciones por acciones no autorizadas

Según lo especificado en la DPC de PKIBDE.

5.3.7 Requisitos de contratación de terceros

Según lo especificado en la DPC de PKIBDE.

5.3.8 Documentación proporcionada al personal

Según lo especificado en la DPC de PKIBDE.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

Según lo especificado en la DPC de PKIBDE.

5.4.2 Frecuencia de procesado de registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.3 Periodo de conservación de los registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.4 Protección de los registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Según lo especificado en la DPC de PKIBDE.

5.4.6 Sistema de recogida de información de auditoría (interno vs externo)

Según lo especificado en la DPC de PKIBDE.

5.4.7 Notificación al sujeto causa del evento

Según lo especificado en la DPC de PKIBDE.

5.4.8 Análisis de vulnerabilidades

Según lo especificado en la DPC de PKIBDE.

5.5 Archivo de registros

5.5.1 Tipo de eventos archivados

Según lo especificado en la DPC de PKIBDE.

5.5.2 Periodo de conservación de registros

Según lo especificado en la DPC de PKIBDE.

5.5.3 Protección del archivo

Según lo especificado en la DPC de PKIBDE.

5.5.4 Procedimientos de copia de respaldo del archivo

Según lo especificado en la DPC de PKIBDE.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Según lo especificado en la DPC de PKIBDE.

5.5.6 Sistema de archivo de información de auditoría (interno vs externo)

Según lo especificado en la DPC de PKIBDE.

5.5.7 Procedimientos para obtener y verificar información archivada

Según lo especificado en la DPC de PKIBDE.

5.6 Cambio de claves de una AC

Según lo especificado en la DPC de PKIBDE.

5.7 Recuperación en caso de compromiso de una clave o catástrofe

5.7.1 Procedimientos de gestión de incidentes y compromisos

Según lo especificado en la DPC de PKIBDE.

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

Según lo especificado en la DPC de PKIBDE.

5.7.3 Procedimiento de actuación ante el compromiso de la clave privada de una Autoridad

Según lo especificado en la DPC de PKIBDE.

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

Según lo especificado en la DPC de PKIBDE.

5.8 Cese de una AC o AR

5.8.1 Autoridad de Certificación

Según lo especificado en la DPC de PKIBDE.

5.8.2 Autoridad de Registro

No estipulado.

6 Controles de seguridad técnica

Los controles de seguridad técnica para los componentes internos de PKIBDE, y concretamente para AC Raíz y AC Corporativa en los procesos de emisión y firma de certificados, están descritos en la DPC de PKIBDE.
En este apartado se recogen los controles de seguridad técnica para la emisión de certificados bajo esta PC.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Las claves para los certificados de emitidos por la AC Corporativa bajo esta PC son generadas de acorde a las siguientes circunstancias, que dependen del tipo de certificado:

Certificados personales

- Certificado de autenticación: las claves se generan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.
- Certificado de firma electrónica: las claves se generan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.
- Certificados de cifrado (obsoleto) y de cifrado recuperable en software: las claves son generadas por la AC Corporativa en módulos de hardware criptográficos con certificación FIPS 140-2 Level 3.

Certificados de administrador: las claves se generan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.

Certificados provisionales personales

- Certificado provisional de autenticación: las claves se generan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.
- Certificado provisional de firma electrónica: las claves se generan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.

Certificados provisionales de administrador: las claves se generan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.

6.1.2 Entrega de la clave privada al titular

Según se describe en el apartado 6.1.1, todas las claves privadas, salvo las correspondientes a los certificados de cifrado (obsoleto) y de cifrado recuperables en software, se generan en un dispositivo criptográfico, por lo que no se requiere entrega al titular.

En cuanto a la entrega de las claves privadas de cifrado, el proceso depende del tipo de certificado de cifrado asociado:

- Certificado de cifrado (obsoleto): las claves se entregan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente.
- Certificado de cifrado recuperable en software: las claves se entregan en un dispositivo criptográfico (típicamente tarjeta criptográfica), que ha de cumplimentar las especificaciones FIPS 140-2 Level 3 o CC EAL4+ o equivalente. Adicionalmente, el usuario podrá recuperar copia de la clave privada en formato PKCS#12, típicamente para su importación en un dispositivo móvil.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública la genera la propia AC Corporativa, por lo que no procede esta entrega.

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

La clave pública de la AC Corporativa está incluida en el certificado de dicha AC. El certificado de la AC Corporativa no viene incluido en el certificado generado para el titular. El certificado de la AC Corporativa 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.

6.1.5 Tamaño de las claves

El tamaño mínimo de las claves de los certificados de usuario interno es de 2048 bits, si bien se admite el uso de certificados de cifrado (obsoletos) de 1024 bits.

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

La clave pública de los certificados de usuario interno está codificada de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es el RSA.

6.1.7 Fines del uso de la clave (campo KeyUsage de X.509 v3)

El valor de los atributos *Key Usage* y *Extended Key Usage* está descrito en el apartado 7.1.2.

6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos

6.2.1 Estándares para los módulos criptográficos

El módulo utilizado para la creación de claves utilizadas por la AC Corporativa de PKIBDE tiene la certificación FIPS 140-2 Level 3.

La puesta en marcha de cada una de las Autoridades de Certificación, contando con 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, aptas como dispositivos seguros de creación de firma, cumplen el nivel de seguridad CC EAL4+, aunque también son admisibles las certificaciones equivalentes ITSEC E3 o FIPS 140-2 Nivel 2.

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 cuya activación se realiza mediante la inicialización del software de AC por medio de

una combinación de operadores de la AC. Éste es el único método de activación de dicha clave privada.
No se establece control multipersona para el acceso a las claves privadas que se almacenan en tarjetas criptográficas de los certificados emitidos bajo esta PC. En cuanto a la copia de las claves privadas almacenadas en el Archivo de Claves por parte de una persona distinta del titular, se exige la intervención de dos personas: una para recuperar la clave en formato PKCS#12 y otra para introducir el PIN que lo protege. En el apartado 4.12.1 se describe este procedimiento.

6.2.3 Custodia de la clave privada

Las claves privadas de los certificados de usuario interno se encuentran alojadas en tarjetas criptográficas, no siendo posible su exportación una vez instaladas en ningún caso y estando protegido el acceso a las operaciones con las mismas mediante PIN.
La única excepción radica en las claves privadas de los certificados de cifrado (obsoletos) y de los certificados de cifrado recuperables en software. En este caso, la AC Corporativa, una vez generado el par de claves, guarda cifrada la clave privada de cifrado en el Archivo de Claves, que utiliza un módulo criptográfico de seguridad (HSM) para protegerla. La recuperación de una clave privada de cifrado del Archivo de Claves está descrita en el apartado 4.12.1.

6.2.4 Copia de seguridad de la clave privada

Los titulares de certificados emitidos bajo esta PC, no pueden realizar copias de seguridad de sus certificados puesto que las claves no pueden ser exportadas de las tarjetas y éstas no son clonables.
La única excepción radica en las claves privadas de los certificados de cifrado recuperables en software. El titular del certificado no requiere realizar una copia de seguridad de la clave privada, ya que podrá recuperarla del Archivo de Claves en todo momento.

6.2.5 Archivo de la clave privada

La AC Corporativa una vez finalizado el proceso de emisión del certificado de usuario interno, no conserva copia de su clave privada, de forma que la clave privada únicamente se encuentra en la correspondiente tarjeta criptográfica del titular.
La única excepción radica en las claves privadas de los certificados de cifrado (obsoletos) y de los certificados de cifrado recuperables en software. En este caso, la AC Corporativa, una vez generado el par de claves, guarda cifrada la clave privada de cifrado en el Archivo de Claves, que utiliza un módulo criptográfico de seguridad (HSM) para protegerla. La recuperación de una clave privada de cifrado del Archivo de Claves está descrita en el apartado 4.12.1.

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

No estipulado.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se crean en la tarjeta criptográfica y se conservan en la misma.
La única excepción radica en las claves privadas de los certificados de cifrado (obsoletos) y de los certificados de cifrado recuperables en software. En este caso la AC Corporativa genera las claves con un módulo criptográfico de seguridad (HSM), y posteriormente envía copia al Archivo de Claves, que también utiliza un HSM para protegerla. La recuperación de una clave privada de cifrado del Archivo de Claves está descrita en el apartado 4.12.1.

6.2.8 Método de activación de la clave privada

Las claves privadas de los certificados de usuario interno se almacenan en un dispositivo criptográfico (típicamente una tarjeta criptográfica) y su uso se controla mediante la introducción del PIN del dispositivo.

La única excepción radica en las claves privadas de los certificados de cifrado recuperables en software. En este caso, la protección de la clave privada depende de las capacidades proporcionadas por el dispositivo en el que se almacene (típicamente un dispositivo móvil)

6.2.9 Método de desactivación de la clave privada

Se puede desactivar retirando la tarjeta del lector. Algunas aplicaciones informáticas también facilitan su desactivación tras un tiempo de inactividad.

La única excepción radica en las claves privadas de los certificados de cifrado recuperables en software. En este caso, la desactivación de la clave privada depende de las capacidades proporcionadas por el dispositivo en el que se almacene (típicamente un dispositivo móvil)

6.2.10 Método de destrucción de la clave privada

Según lo especificado en la DPC de PKIBDE.

6.2.11 Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 Level 3 o CC EAL4+ o equivalente.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

Según lo especificado en la DPC de PKIBDE.

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

Los certificados de usuario interno, así como los pares de claves asociados, tienen un periodo de uso de 4 años, si bien en el momento de su emisión la AC Corporativa puede establecer periodos inferiores.

La única excepción radica en los certificados provisionales (tanto personales como de administrador), así como los pares de claves asociados, que tienen un periodo de uso máximo de 7 días, si bien en el momento de su emisión la AC Corporativa puede establecer periodos inferiores.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Según lo especificado en la DPC de PKIBDE.

6.4.2 Protección de los datos de activación

Según lo especificado en la DPC de PKIBDE.

6.4.3 Otros aspectos de los datos de activación

Según lo especificado en la DPC de PKIBDE.

6.5 Controles de seguridad informática

6.5.1 Requerimientos técnicos de seguridad específicos

Según lo especificado en la DPC de PKIBDE.

6.5.2 Evaluación de la seguridad informática

Según lo especificado en la DPC de PKIBDE.

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Según lo especificado en la DPC de PKIBDE.

6.6.2 Controles de gestión de seguridad

Según lo especificado en la DPC de PKIBDE.

6.6.3 Controles de seguridad del ciclo de vida

Según lo especificado en la DPC de PKIBDE.

6.7 Controles de seguridad de la red

Según lo especificado en la DPC de PKIBDE.

6.8 Sellado de tiempo

Según lo especificado en la DPC de PKIBDE.

7 Perfiles de los Certificados, CRL y OCSP

7.1 Perfil de Certificado

7.1.1 Número de versión

Los certificados de componente de uso interno emitidos por la AC Corporativa utilizan el estándar X.509 versión 3 (X.509 v3).

7.1.2 Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- *Subject Key Identifier*. Calificada como no crítica.
- *Authority Key Identifier*. Calificada como no crítica.
- *KeyUsage*. Calificada como crítica.
- *extKeyUsage*. Calificada como no crítica.
- *CertificatePolicies*. Calificada como no crítica.
- *SubjectAlternativeName*. Calificada como no crítica.
- *BasicConstraints*. Calificada como crítica.
- *CRLDistributionPoint*. Calificada como no crítica.
- *Auth. Information Access*. Calificada como no crítica.
- *bdeCertType (1.3.6.1.4.1.19484.2.3.6)*. Calificada como no crítica.

7.1.2.1 Certificado de autenticación

Certificado de autenticación		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	En el caso de empleados del Banco de España CN=[A] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES En el caso de personal de empresas contratadas CN=[A] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS OU=EMPRESAS EXTERNAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud minima clave: 2048(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, smartCardLogon, anyExtendedKeyUsage, emailProtection[10]	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	

[10]Este atributo sólo se incluirá en los certificados personales de autenticación que emita PKIBDE para el personal de empresas contratadas.

Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.6	
Notice Reference	Certificado personal de autenticación sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	UPN (User´s Principal Name de Windows 2000) Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[11]	NO
7. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	AUTENTICACION	

[11] Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.2.2 Certificado de firma electrónica

Certificado de firma electrónica		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	CN=[F] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud minima clave: 2048(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	0	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	emailProtection, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado Reconocido según la legislación vigente. Uso sujeto a la DPC del Banco de España. © 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.12	
Notice Reference	Certificado personal de firma electrónica sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. qcStatements	Id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1)	
7. Subject Alternate Names	Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1	NO

	1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación	
8. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
9. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
10. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
11. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	FIRMA	

7.1.2.3 Certificado de cifrado recuperable en software

Certificado de cifrado recuperable en software		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncrytion	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	En el caso de empleados del Banco de España CN=[C] Nombre Apellido1 Apellido 2 SerialNumber=NIF PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES En el caso de personal de empresas contratadas CN=[C] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS OU=EMPRESAS EXTERNAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	emailProtection, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.17	

Notice Reference	Certificado personal de cifrado recuperable en software sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[12]	NO
7. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	CIFRADO	

[12]Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.2.4 Certificado de cifrado (obsoleto)

Certificado de cifrado (obsoleto)		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-1WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	En el caso de empleados del Banco de España CN=[C] Nombre Apellido1 Apellido 2 SerialNumber=NIF PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES En el caso de personal de empresas contratadas CN=[C] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS OU=EMPRESAS EXTERNAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 1024(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		NO
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora (AC-CORPORATIVA) (c2 45 2b f4 f9 92 ee 33 59 98 e1 82 75 6b 8c bc d0 b6 e5 c1)	
authorityCertIssuer	CN=BANCO DE ESPAÑA-AC RAIZ, O=BANCO DE ESPAÑA C=ES	
authorityCertSerialNumber	36 6a 52 4d a5 e4 4a f8 41 08 a1 40 9b 9b 76 eb	
3. KeyUsage		SI
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	emailProtection, anyExtendedKeyUsage	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del	

	Banco de España. © 2014 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.8	
Notice Reference	Certificado personal de cifrado sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2014 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[13]	NO
7. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20 DE%20ESPA%D1A%20-%20AC%20CORPORATIVA,CN=snt0053,CN=CDP, CN=Public%20Key%20Services,CN=Services,CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList?base?objectclass= cRLDistributionPoint (2) LDAP: ldap://pkildap.bde.es/CN=CRL,CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA, CN=Internas, CN=PKI, CN=Configuration, DC=BDE, DC=ES ?certificateRevocationList ?base ?objectclass=cRLDistributionPoint (3)HTTP http://pki.bde.es/certs/ACcorporativa.crl	NO
9. Auth. Information Access	OCSP http://pkiva.bde.es CA http://pki.bde.es/certs/ACraiz.crt	NO
10.netscapeCertType	SMIMEClient	
11. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	CIFRADO	

[13]Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.2.5 Certificado de administrador

Certificado de administrador		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	4 años	
6. Subject	En el caso de empleados del Banco de España CN=[X] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES En el caso de personal de empresas contratadas CN=[X] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS OU=EMPRESAS EXTERNAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud minima clave: 2048(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, smartCardLogon, anyExtendedKeyUsage, emailProtection	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	

Policy Identifier	1.3.6.1.4.1.19484.2.2.15	
Notice Reference	Certificado de administrador sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	UPN (User´s Principal Name de Windows 2000) Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[14]	NO
7. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	ADMINISTRADOR	

[14]Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.2.6 Certificado provisional de autenticación

Certificado de provisional de autenticación		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	7 días (valor máximo)	
6. Subject	En el caso de empleados del Banco de España CN=[A] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES En el caso de personal de empresas contratadas CN=[A] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS OU=EMPRESAS EXTERNAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud minima clave: 2048(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, smartCardLogon, anyExtendedKeyUsage, emailProtection[15]	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	

[15]Este atributo sólo se incluirá en los certificados personales de autenticación que emita PKIBDE para el personal de empresas contratadas.

Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.13	
Notice Reference	Certificado provisional de autenticación sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	UPN (User´s Principal Name de Windows 2000) Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[16]	NO
7. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	AUTENTICACION-PROVISIONAL	

[16]Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.2.7 Certificado provisional de firma electrónica

Certificado de provisional de firma electrónica		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	7 días (valor máximo)	
6. Subject	CN=[F] Nombre Apellido1 Apellido 2 serialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 1024 (big string) a 2048	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	0	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	emailProtection, anyExtendedKeyUsage	
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado Reconocido según la legislación vigente. Uso sujeto a la DPC del Banco de España. @2015 Banco de España. Todos los derechos reservados (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.10	
Notice Reference	Certificado personal de firma provisional sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. qcStatements	id-qcs-pkixQCSyntax-v1 (certificado reconocido) id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1)	NO
7. Subject Alternate Names	Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1	

	1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE 1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[17]		
8. Basic Constraints	CA	SI	
Subject Type			
Path Length Constraint	No utilizado		
9. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl		NO
10. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt		NO
11. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	FIRMA-PROVISIONAL		

[17] Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.2.8 Certificado provisional de administrador

Certificado de provisional de administrador		
CAMPO	**CONTENIDO**	**CRÍTICA para extensiones**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA-256WithRSAEncryption	
4. Issuer Distinguished Name	CN=BANCO DE ESPAÑA – AC CORPORATIVA V2, O=BANCO DE ESPAÑA, C=ES	
5. Validez	7 días (valor máximo)	
6. Subject	CN=[X] Nombre Apellido1 Apellido 2 SerialNumber= Documento Identificación PS=Código Usuario OU=PERSONAS O=BANCO DE ESPAÑA C=ES	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud minima clave: 2048(big string)	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Authority Key Identifier		
keyIdentifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la AC emisora: 31 ed f3 61 80 c8 49 dc d6 cc 3d 0c e6 28 e2 5c 60 53 dd 58	
3. KeyUsage		SI
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, smartCardLogon, anyExtendedKeyUsage, emailProtection	NO
5. Certificate Policies		NO
Policy Identifier	1.3.6.1.4.1.19484.2.2.1	
URL CPS	http://pki.bde.es/politicas	
Notice Reference	Certificado sujeto a: Declaración de Prácticas de Certificación del Banco de España. © 2015 Banco de España. Todos los derechos reservados. (C/Alcalá 48, 28014 Madrid-España)	
Policy Identifier	1.3.6.1.4.1.19484.2.2.16	
Notice Reference	Certificado provisional de administrador sujeto a la Declaración de Prácticas de Certificación del Banco de España. ©2015 Banco de España. Todos los derechos reservados	
6. Subject Alternate Names	UPN (User´s Principal Name de Windows 2000) Dirección email según RFC 822 1.3.6.1.4.1.19484.2.3.1 Nombre 1.3.6.1.4.1.19484.2.3.2 Apellido1 1.3.6.1.4.1.19484.2.3.3 Apellido2 1.3.6.1.4.1.19484.2.3.4 Nº de empleado BDE 1.3.6.1.4.1.19484.2.3.5 Código Usuario BDE	NO

	1.3.6.1.4.1.19484.2.3.7 Documento Identificación 1.3.6.1.4.1.19484.2.3.15 Id. para subcontratados[18]	
7. Basic Constraints	CA	SI
Subject Type	Entidad Final	
Path Length Constraint	No utilizado	
8. CRLDistributionPoints	(1) Directorio Activo: ldap:///CN=BANCO%20DE%20ESPA%D1A-AC%20CORPORATIVA%20V2,CN=PKIBDE,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=BDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint (2) HTTP 1: http://pki.bde.es/crls/ACcorporativav2.crl (3)HTTP 2: http://pki.redbde.es/crls/ACcorporativav2.crl	NO
9. Auth. Information Access	OCSP 1: http://ocsp.bde.es OCSP 2: http://ocsp-pkibde.es.escb.eu CA: http://pki.bde.es/certs/ACraizv2.crt	NO
10. bdeCertType (1.3.6.1.4.1.19484.2.3.6)	ADMINISTRADOR-PROVISIONAL	

[18]Este atributo sólo se incluirá en los certificados personales que emita PKIBDE para el personal de empresas contratadas. Permite diferenciar a los titulares que pertenecen a este colectivo.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) de los algoritmos Criptográficos:

- SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)

7.1.4 Formatos de nombres

Los certificados emitidos por PKIBDE contienen el Distinguished Name X.500 del emisor y el del destinatario del certificado en los campos issuer name y subject name respectivamente.

7.1.5 Restricciones de los nombres

Ver la sección 3.1.1.

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

El OID de la presente PC es 1.3.6.1.4.1.19484.2.2.20. Se añade una extensión de formato X.Y que recoge la versión de la PC.

Los OIDs de los certificados regulados por esta política son los siguientes:

- 1.3.6.1.4.1.19484.2.2.6: Política de Certificación para certificados de autenticación
- 1.3.6.1.4.1.19484.2.2.12: Política de Certificación para certificados de firma electrónica
- 1.3.6.1.4.1.19484.2.2.17: Política de Certificación para certificados de cifrado recuperables en software
- 1.3.6.1.4.1.19484.2.2.8: Política de Certificación para certificados de cifrado (obsoleta)
- 1.3.6.1.4.1.19484.2.2.15: Política de Certificación para certificados de administrador
- 1.3.6.1.4.1.19484.2.2.13: Política de Certificación para certificados provisionales de autenticación
- 1.3.6.1.4.1.19484.2.2.10: Política de Certificación para certificados provisionales de firma electrónica
- 1.3.6.1.4.1.19484.2.2.16: Política de Certificación para certificados provisionales de administrador

7.1.7 Uso de la extensión "PolicyConstraints"

No estipulado.

7.1.8 Sintaxis y semántica de los "PolicyQualifier

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

- URL CPS: contiene la URL a la DPC y a la PC que rigen el certificado.
- Notice Referente: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

Dentro del apartado *7.1.2 Extensiones del certificado* se puede ver su contenido para los certificados regulados por esa política.

7.1.9 Tratamiento semántico para la extensión critica "CertificatePolicy"

No estipulado.

7.2 Perfil de CRL

7.2.1 Número de versión

Según lo especificado en la DPC de PKIBDE.

7.2.2 CRL y extensiones

Según lo especificado en la DPC de PKIBDE.

7.3 Perfil de OCSP

7.3.1 Número(s) de versión

Según lo especificado en la DPC de PKIBDE.

7.3.2 Extensiones OCSP

Según lo especificado en la DPC de PKIBDE.

8 Auditorías de cumplimiento y otros controles

8.1 Frecuencia o circunstancias de los controles para cada Autoridad

Según lo especificado en la DPC de PKIBDE.

8.2 Identificación/cualificación del auditor

Según lo especificado en la DPC de PKIBDE.

8.3 Relación entre el auditor y la Autoridad auditada

Según lo especificado en la DPC de PKIBDE.

8.4 Aspectos cubiertos por los controles

Según lo especificado en la DPC de PKIBDE.

8.5 Acciones a tomar como resultado de la detección de deficiencias

Según lo especificado en la DPC de PKIBDE.

8.6 Comunicación de resultados

Según lo especificado en la DPC de PKIBDE.

9 Otras cuestiones legales y de actividad

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

No se aplica ninguna tarifa sobre la emisión o renovación de certificados bajo el amparo de la presente Política de Certificación.

9.1.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos bajo esta Política es gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

9.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

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 Confidencialidad de la información

9.2.1 Ámbito de la información confidencial

Según lo especificado en la DPC de PKIBDE.

9.2.2 Información no confidencial

Según lo especificado en la DPC de PKIBDE.

9.2.3 Deber de secreto profesional

Según lo especificado en la DPC de PKIBDE.

9.3 Protección de la información personal

9.3.1 Política de protección de datos de carácter personal

Según lo especificado en la DPC de PKIBDE.

9.3.2 Información tratada como privada

Según lo especificado en la DPC de PKIBDE.

9.3.3 Información no calificada como privada

Según lo especificado en la DPC de PKIBDE.

9.3.4 Responsabilidad de la protección de los datos de carácter personal

Según lo especificado en la DPC de PKIBDE.

9.3.5 Comunicación y consentimiento para usar datos de carácter personal

Según lo especificado en la DPC de PKIBDE.

9.3.6 Revelación en el marco de un proceso judicial

Según lo especificado en la DPC de PKIBDE.

9.3.7 Otras circunstancias de publicación de información

Según lo especificado en la DPC de PKIBDE.

9.4 Derechos de propiedad Intelectual

Según lo especificado en la DPC de PKIBDE.

9.5 Obligaciones

9.5.1 Obligaciones de la AC

Según lo especificado en la DPC de PKIBDE.

La Autoridad de Certificación Corporativa de PKIBDE actuará relacionando una determinada clave pública con su titular mediante la emisión de un certificado electrónico, todo ello de conformidad con los términos de esta PC y de la DPC.

Los servicios prestados por la AC en el contexto de esta PC son los servicios de emisión, renovación y revocación de certificados de usuario interno, a los que se accede mediante los Puestos de Administración remotos de la AC desplegados a tal efecto.

9.5.2 Obligaciones de la AR

Según lo especificado en la DPC de PKIBDE.

9.5.3 Obligaciones de los titulares de los certificados

Según lo especificado en la DPC de PKIBDE.

9.5.4 Obligaciones de los terceros aceptantes

Según lo especificado en la DPC de PKIBDE.

9.5.5 Obligaciones de otros participantes

Según lo especificado en la DPC de PKIBDE.

9.6 Responsabilidades

9.6.1 Responsabilidades de PKIBDE

Según lo especificado en la DPC de PKIBDE.

9.6.2 Exención de responsabilidades de PKIBDE

Según lo especificado en la DPC de PKIBDE.

9.6.3 Alcance de la cobertura

Según lo especificado en la DPC de PKIBDE.

9.7 Limitaciones de pérdidas

Según lo especificado en la DPC de PKIBDE.

9.8 Periodo de validez

9.8.1 Plazo

Esta PC entrará en vigor desde el momento de su aprobación por la AAP y su publicación en el repositorio de PKIBDE.

Esta PC está en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC Corporativa, ocasión en que obligatoriamente se emitirá una nueva versión.

9.8.2 Sustitución y derogación de la PC

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

Cuando la PC quede derogada se retirará del repositorio público de PKIBDE, si bien se conservará durante 15 años.

9.8.3 Efectos de la finalización

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

9.9 Notificaciones individuales y comunicaciones con los participantes

Según lo especificado en la DPC de PKIBDE.

9.10 Procedimientos de cambios en las especificaciones

9.10.1 Procedimiento para los cambios

Según lo especificado en la DPC de PKIBDE.

9.10.2 Periodo y mecanismo de notificación

Según lo especificado en la DPC de PKIBDE.

9.10.3 Circunstancias en las que el OID debe ser cambiado

Según lo especificado en la DPC de PKIBDE.

9.11 Reclamaciones y jurisdicción

Según lo especificado en la DPC de PKIBDE.

9.12 Normativa aplicable

Según lo especificado en la DPC de PKIBDE.

9.13 Cumplimiento de la normativa aplicable

Según lo especificado en la DPC de PKIBDE.

9.14 Estipulaciones diversas

9.14.1 Cláusula de aceptación completa

Según lo especificado en la DPC de PKIBDE.

9.14.2 Independencia

En el caso que una o más estipulaciones de esta PC 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 PC careciera ésta de toda eficacia jurídica.

9.14.3 Resolución por la vía judicial

No estipulado.

9.15 Otras estipulaciones

No estipulado

10 Protección de datos de carácter personal

10.1 Régimen jurídico de protección de datos

Según lo especificado en la DPC de PKIBDE.

10.2 Creación del fichero e inscripción registral

Según lo especificado en la DPC de PKIBDE.

10.3 Documento de seguridad LOPD

Según lo especificado en la DPC de PKIBDE.