Servicio Público de Empleo Estatal

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

OID: 1.3.6.1.4.1.27781.1.2.1.1.1

Versión 1.3

Fecha: 19 de Julio de 2012

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Índice

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 1. Introducción

1.1. Objeto

El presente documento recoge la Declaración de Prácticas de Certificación de la Autoridad de Certificación, en adelante AC, del Servicio Público de Empleo Estatal, en adelante SEPE, que define los mecanismos y procedimientos para la emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida de los certificados electrónicos emitidos por la AC del SEPE.

La Declaración de Prácticas de Certificación (en adelante DPC) del SEPE se ha estructurado conforme al documento RFC-3647 *"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" o "No Aplica".

En cuanto al marco legislativo, se han seguido estas normativas:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

La DPC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía en la relación entre el SEPE y los usuarios de sus servicios telemáticos.

Todas las partes involucradas tienen la obligación de conocer esta DPC y ajustar su actividad a lo dispuesto en la misma.

1.2. Tipos y clases de certificados

La Autoridad de Certificación del SEPE emite diferentes tipos de certificados:

- Certificados de Ciudadano, que son emitidos a ciudadanos que estén en disposición de realizar trámites en el portal de Sede Electrónica que requiera firma digital.

En el futuro, el SEPE se reserva el derecho de emitir nuevos tipos de certificados o cesar la emisión de los ya existentes.

1.3. Relación entre la Declaración de Prácticas de Certificación y otros documentos

Este documento contiene la Declaración de Prácticas de Certificación (DPC) de la AC del SEPE. Cada uno de los tipos de certificado que emita tendrá su correspondiente Política de Certificación.

Esta DPC incluye los procedimientos que aplica en la prestación de sus servicios, en cumplimiento de los requisitos establecidos por las políticas que gestiona y el artículo 19 de la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica.

1.4. Nombre e Identificación del documento

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Nombre del documento	SEPE. Declaración de Practicas de Certificación
Versión del documento	1.1
Estado del documento	Aprobado
Fecha de emisión	16/11/2011
OID (Object Identifier)	1.3.6.1.4.1.27781.1.2.1.1.1
Ubicación de la DPC	http://sede.sepe.gob.es/dpc

1.5. Participantes

1.5.1. Autoridades de Certificación

La AC del SEPE proporciona servicios de expedición y gestión de certificados de ciudadano. Los datos fundamentales del certificado raíz de la AC son los siguientes:

Nombre Distintivo	OU=AC SPEE, O=SPEE, C=ES
Certificado pkcs1-sha1WithRSAEncryption	
Número de serie	4adcb600
Periodo de Validez	Desde: lunes, 19 de octubre de 2009 20:24:59 Hasta: jueves, 19 de octubre de 2034 20:54:59
Huella digital (SHA-1)	78 fc 1d 5b 65 b0 e5 a3 e2 10 85 b5 de 50 d6 ec 0b bf 1d cf
Algoritmo de firma	sha1RSA
Clave Pública	RSA (2048)

1.5.2. Autoridades de Registro

La Autoridad de Registro (en adelante RA) del SEPE es la entidad que realiza la comprobación de las solicitudes de certificados y actúa de intermediario entre el usuario de los certificados y la AC.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Actuarán como entidades de registro las unidades, dependencias u oficinas de las Entidades Gestoras y Servicios Comunes del SEPE que se designen al efecto en cada Política de Certificación específica.

1.5.3. Suscriptores

Los suscriptores son los ciudadanos y el propio organismo que obtienen y utilizan certificados emitidos por el SEPE, ya sean de ciudadano.

1.5.4. Partes confiables

No estipulado.

1.5.5. Otros

No estipulado.

1.6. Uso de los Certificados

Existen ciertas limitaciones en el uso de los certificados del SEPE. Un certificado emitido por la AC del SEPE sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta DPC.

1.6.1. Usos apropiados de los certificados del SEPE

Un certificado emitido por la AC del SEPE sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta DPC y en su correspondiente Política de Certificación.

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

1.7. Política de Administración de la DPC

El SEPE se reserva el derecho de hacer revisiones y actualizaciones de sus políticas si así lo estimase oportuno, y es el único organismo autorizado para hacer modificaciones sobre esta DPC.

1.7.1. Organización que administra la DPC

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Nombre	Servicio Público de Empleo Estatal		
Dirección e-mail			
Dirección	C/ Condesa de Venadito 9 28027 – Madrid España		
Teléfono		**Fax**	

1.7.2. Procedimientos de aprobación de la DPC

La Subdirección General de Tecnologías de la Información y Comunicaciones del SEPE acordará por unanimidad las modificaciones de la DPC en curso.

1.7.3. Actualizaciones de la DPC

Tras la aprobación de la DPC, SEPE publicará la misma en la dirección **http://sede.sepe.gob.es/dpc**

1.8. Definiciones y Acrónimos

En el ámbito de esta DPC se utilizan las siguientes definiciones y acrónimos:

Autoridad de Certificación (AC): Autoridad de Certificación. En inglés CA (Certification Authority). Aplicación o programa encargado de la emisión y gestión de certificados y listas de certificados revocados, incluyendo la revocación, suspensión, renovación y desactivación de los mismos. Tercera parte de confianza que acredita la conexión entre una determinada clave pública y su propietario. La confianza en la AC supone la confianza en los certificados que emite.

ARL: Authority Revocation List. Lista de Autoridades de Certificación Revocadas.

Auditoría: Procedimiento usado para verificar que se están llevando a cabo controles en un sistema de información y que estos son adecuados para los objetivos que se persiguen. Incluye el análisis de las actividades para detectar intrusiones o abusos dentro del sistema.

Autenticidad: Característica por la que se garantiza la identidad del usuario que origina un mensaje o transacción, es decir conocer con certeza quién envía algo.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Autenticación: Proceso utilizado para confirmar la identidad y autenticidad de una persona o probar la integridad de información específica.

Autoridad de Registro: Entidad autorizada por la Autoridad de Certificación para registrar a los usuarios de la infraestructura asignándoles un identificador único de usuario.

Certificado: Es un documento electrónico en el cual la Autoridad de Certificación (AC) acredita mediante su firma digital que la clave pública pertenece a su propietario. También se denominan Certificados de usuario y de clave pública.

Clave Privada: Clave personal que no es conocida por el resto de los usuarios y que es utilizada para crear firmas digitales y, dependiendo del algoritmo, para descifrar mensajes cifrados con la correspondiente clave pública.

Clave Pública: Clave de usuario que es conocida por el resto de los usuarios y que es utilizada para verificar firmas creadas con su correspondiente clave pública. Dependiendo del algoritmo, se usa para cifrar mensajes que pueden ser descifrados con su correspondiente clave privada.

Compromiso: Violación (o sospecha de violación) de una política de seguridad, en la cual puede haber ocurrido una revelación no autorizada de información crítica.

Criptografía: Ciencia matemática usada para asegurar la confidencialidad y autenticidad de datos mediante el proceso de reemplazarlos por una versión transformada. Esta puede ser reconvertida a la forma original sólo por alguien que posea el algoritmo criptográfico y las claves adecuadas.

También es el nombre que se le da a la disciplina que incluye los principios, medios y métodos para transformar los datos con intención de ocultar la información y prevenir la modificación y los usos no autorizados de la misma.

CRL: Certificate Revocation List. (Listas de Certificados revocados). Contiene los números de serie de los certificados revocados por la AC.

Declaración de Prácticas de Certificación: Es un documento declarativo donde se describe la política de servicios y los niveles de garantía ofrecidos por la Autoridad de Certificación. De igual manera, supone el marco de relación entre la AC, las entidades relacionadas y sus suscriptores.

Emisión de certificados: Acciones llevadas a cabo por una AC para crear un certificado y comunicárselo al usuario que lo solicitó.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Expiración de un certificado: Fecha y hora especificadas en un certificado cuando termina el periodo operativo del mismo.

Extensión de un certificado: Campo añadido a un certificado para guardar información adicional.

Firma digital / Firma electrónica: Es un documento electrónico que se genera como resultado de aplicar una función matemática al documento a firmar y posteriormente cifrar el resultado con la clave privada del firmante.

Es utilizada por el emisor de un mensaje para identificarse.

Función Hash: Función matemática que asocia valores de un dominio extenso a uno de menor rango. Las asociaciones se hacen aparentemente de forma aleatoria. Se utilizan para traducir un mensaje de forma que partiendo del mismo mensaje y función se obtenga siempre el mismo resultado, sea imposible reconstruir el mensaje original a partir del traducido y, además, sea imposible encontrar dos mensajes distintos que den el mismo resultado con la misma función.

HSM: Hardware Security Module, *Módulo hardware de seguridad*. Dispositivo físico que almacena de forma segura la clave privada de la AC, y realiza de forma segura las operaciones de firma de los certificados de los usuarios de la AC.

Identificador único de certificado: Valor que identifica unívocamente a un certificado.

Infraestructura de clave pública (PKI): Conjunto de mecanismos criptográficos de clave pública basados en la existencia de dos claves (una pública y otra privada) que se utilizan para garantizar la identidad del usuario, la confidencialidad y la integridad de la información transmitida.

Integridad: Característica que asegura que el mensaje o comunicación que se recibe llega tal y como se envió por el remitente, detectando fácilmente posibles modificaciones que pudieran haberse producido durante la transmisión.

ISO/IEC: Organización Internacional de Normalización.

ISO7816: Norma para la fabricación y utilización de tarjetas inteligentes.

ITSEC: Information Technology Security Evaluation Criteria.

Nombre Distintivo (DN): En inglés, *Distinguished Name*: cadena de caracteres que identifica de forma unívoca a un objeto dentro de un repositorio LDAP.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

No repudio: Mecanismos que proporcionan garantías del origen de un mensaje para proteger al emisor contra la negación de recepción por parte del receptor.

Período de validez de un certificado: Periodo que comienza con la emisión del certificado y termina con la fecha de expiración o antes si el certificado es revocado.

Política de seguridad: Documento que recoge todos los requisitos y prácticas de seguridad para asegurar el funcionamiento de la infraestructura de una forma fiable.

Privacidad: Característica que garantiza que nadie salvo el destinatario puede acceder al contenido de un mensaje.

PSC: Prestador de Servicios de Certificación.

Recuperación de datos: Procedimiento de obtención del mensaje original, a partir de un mensaje cifrado, en situaciones de emergencia.

Registrador: Persona con autoridad para registrar usuarios y revocar certificados en la infraestructura de clave pública.

Registro de usuarios: Procedimiento por el que se toman los datos personales de un usuario, se confirma su identidad y se formaliza su contrato con SEPE.

Revocación de certificados: Anulación de la validez de un certificado de clave pública antes del fin del periodo de validez.

Servicios de la Entidad Pública de Certificación: Conjunto de funciones relacionadas que la AC puede ofrecer como soporte de la seguridad a usuarios, a otras Autoridades Certificadoras y como apoyo a otros servicios de la propia Autoridad.

Tercero aceptante: Persona o entidad diferente del titular que decide aceptar y confiar en un certificado emitido por el SEPE.

Validación de un certificado de usuario: Proceso llevado a cabo por una entidad de confianza o el receptor de un mensaje firmado digitalmente para verificar que el certificado era válido y estaba en el periodo operativo en el momento en el que fue creada la firma.

X509: Norma estándar que define un entorno de autentificación y seguridad. Forma parte de la norma X.500 de UIT -T.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 2. Responsabilidad de publicación y de repositorio

2.1. Repositorios

Toda la información publicada relacionada con esta DPC estará disponible a través de la Sede Electrónica del SEPE (**http://sede.sepe.gob.es/**).

2.2. Publicación de Información de Certificados

El contenido de esta DPC, junto con las Políticas de Certificación para cada tipo de certificado estará disponible en forma de libre acceso en la Sede Electrónica del SEPE (**http://sede.sepe.gob.es/dpc**).

Nuevas versiones del documento se publicarán en la dirección web indicada con anterioridad para la publicación del DPC, sustituyendo a la versión anterior.

2.3. Frecuencia de publicación

La DPC (este documento) y las Políticas de Certificación asociadas, se publicarán en el momento de su creación y de acuerdo a la política de actualización de los mismos, según las modificaciones que se realicen sobre la misma.

2.4. Controles de Acceso a los repositorios

La AC del SEPE establece controles para mantener la integridad de su repositorio interno, de forma tal que:

- Se pueda comprobar la autenticidad de los certificados.
- Las personas no autorizadas no pueden alterar los datos.
- Los certificados solamente están accesibles en los supuestos o a las personas que el firmante indique.
- Detecte cualquier cambio técnico que afecte a los requisitos de seguridad.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 3. Identificación y Autenticación

3.1. Nombres

3.1.1. Tipos de Nombres

Los certificados emitidos por la AC del SEPE contienen el nombre distintivo (DN) del emisor y el titular del certificado en los campos "*Issuer Name*" y "*Subject Name*", respectivamente.

El nombre distintivo del "*Issuer Name*" contiene los siguientes campos:

OU = AC SPEE

O = SPEE

C = ES

La nomenclatura para cada tipo de certificado viene especificada en la correspondiente Política de Certificación.

3.1.2. Necesidades de nombres significativos

Las normas seguidas por esta DPC y las correspondientes Políticas de Certificación garantizan que los nombres distintivos (DN) de los certificados son significativos para asociar de forma inequívoca la clave pública del certificado con una identidad única.

3.1.3. Anonimato o alias de los titulares

No estipulado.

3.1.4. Interpretación del formato de nombres

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

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

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

atributos DirectoryString de los campos Issuer (Emisor) y Subject (Asunto). En los certificados emitidos por la Autoridad de Certificación del SEPE, los atributos de dichos campos están codificados en formato UTF8String.

3.1.5. Unicidad de nombres

El nombre distintivo de los certificados emitidos por la AC del SEPE será único e inequívoco.

3.1.6. Reconocimiento, autenticación y funciones de las marcas registradas

No estipulado.

3.2. Autenticación inicial de la identidad

3.2.1. Métodos de prueba de la posesión de la clave privada

Debido a que el procedimiento de generación del par de claves depende del tipo de certificado emitido, la prueba de posesión de la clave privada se describirá en cada política de certificación específica.

La clave privada de la AC se genera de forma segura en un módulo hardware criptográfico (HSM), compatible con la normativa FIPS-140 nivel 2, y en ningún momento sale del mismo.

3.2.2. Autenticación de la identidad de una organización

La autenticación de la identidad para certificados de organización se especifica en la correspondiente Política de Certificación.

3.2.3. Autenticación de la identidad de ciudadano

La autenticación de la identidad para certificados de ciudadano se especifica en la correspondiente Política de Certificación.

3.2.4. Información no verificada sobre el solicitante

No estipulado.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

3.2.5. Validación de las facultades de representación

No estipulado.

3.2.6. Criterios de interoperabilidad con AC externas

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

3.3. Identificación y autenticación en las peticiones de renovación de claves y certificados

3.3.1. Identificación y autenticación

Este apartado es dependiente del tipo de certificado en particular y está recogido en su correspondiente Política de Certificación.

3.3.2. Identificación y autenticación para la renovación de las claves después de una revocación

Este apartado es dependiente del tipo de certificado en particular y está recogido en su correspondiente Política de Certificación.

3.4. Identificación y autenticación para las peticiones de revocación de certificados

Este apartado es dependiente del tipo de certificado en particular y está recogido en su correspondiente Política de Certificación.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 4. Requisitos del ciclo de vida de los certificados

4.1. Solicitud de los certificados

4.1.1. Quién puede realizar una petición de certificado

Este apartado es dependiente del tipo de certificado en particular y está recogido en su correspondiente Política de Certificación.

4.1.2. Registro de las solicitudes de certificados

Este apartado es dependiente del tipo de certificado en particular y está recogido en su correspondiente Política de Certificación.

4.2. Tramitación de solicitud de certificados

4.2.1. Procedimientos para la identificación y funciones de autenticación

Para cualquier aspecto específico de la identificación y autenticación de los usuarios se remite a la Política de Certificación correspondiente a cada tipo de certificado.

4.2.2. Aprobación o denegación de la solicitud de certificados

Las condiciones para la aprobación o denegación de las solicitudes de certificados, se establecerán en la Política de Certificación correspondiente a cada tipo de certificado.

4.2.3. Plazo para procesar la solicitud de certificado

No estipulado.

4.3. Emisión de certificados

4.3.1. Procedimiento para la emisión del certificado

La emisión del certificado tiene lugar una vez que la AC ha llevado a cabo las comprobaciones necesarias para validar la solicitud de certificación.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Los certificados se emiten automáticamente al recibir una solicitud válida. Los trámites a seguir para la emisión de las claves y certificados de cada tipo se describen en la correspondiente Política de Certificación.

Todos los certificados iniciarán su vigencia en el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.

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

No estipulado.

4.4. Aceptación del certificado

4.4.1. Procedimientos para la aceptación del certificado

El procedimiento para la aceptación del certificado depende del tipo del mismo, y está descrito en la correspondiente Política de Certificación.

4.4.2. Publicación del certificado

No estipulado.

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

No estipulado.

4.5. Par de claves y uso del certificado

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

Los certificados solamente podrán ser utilizados para los usos descritos en la presente DPC y en las correspondientes Políticas de Certificación.

Tras la extinción de la vigencia o la revocación del certificado, el titular deberá dejar de utilizar la clave privada asociada, y los correspondientes certificados.

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

No aplica.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

4.6. Renovación de certificados sin cambio de claves

4.6.1. Circunstancias para la renovación de certificados sin cambio de claves

En el ámbito de la AC del SEPE no se realizará renovación de certificados sin cambio de claves.

4.7. Renovación de certificados con cambio de clave

4.7.1. Motivos para la renovación con cambio de claves de un certificado

Las condiciones particulares de renovación dependen del tipo de certificado en concreto y se especifican en la correspondiente Política de Certificación.

4.7.2. Quién puede solicitar la renovación de un certificado

Esta información se especifica en la Política de Certificación correspondiente al tipo de certificado.

4.7.3. Tratamiento de la solicitud de renovación del certificado

Esta información se especifica en la Política de Certificación correspondiente al tipo de certificado.

4.7.4. Notificación de la emisión del nuevo certificado al titular

Esta información se especifica en la Política de Certificación correspondiente al tipo de certificado.

4.7.5. Procedimientos para la aceptación de los certificados

Esta información se especifica en la Política de Certificación correspondiente al tipo de certificado.

4.7.6. Publicación del certificado tras su renovación

No estipulado.

4.7.7. Notificación de la emisión del certificado a otras entidades

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

No estipulado.

4.8. Modificación de certificados

No aplica.

4.9. Revocación y suspensión de certificados

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible.

La suspensión, en cambio, supone la pérdida de validez temporal de un certificado, y es reversible.

4.9.1. Causas de revocación de certificados

Los motivos por los cuales puede procederse a la revocación de un certificado, se describen en la Política de Certificación correspondiente a cada tipo de certificado.

4.9.2. ¿Quién puede presentar la solicitud de revocación?

En el ámbito de la AC del SEPE pueden solicitar la revocación de un certificado:

- El titular a nombre del cual el certificado fue emitido.
- La Entidad de Registro que intervino en la emisión.
- Servicio Público de Empleo Estatal.

4.9.3. Procedimiento de solicitud de revocación

Los procedimientos para solicitar la revocación de certificados se describen en la Política de Certificación correspondiente.

4.9.4. Efectos de la revocación

La revocación de un certificado implica la imposibilidad de su uso para operaciones de firma.

4.9.5. Plazo para la tramitación de la solicitud de revocación

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

La solicitud de revocación deberá ser tratada en el menor tiempo posible, evitando así el uso fraudulento de certificados emitidos por la AC del SEPE.

4.9.6. Requisitos de verificación de las revocaciones por los terceros aceptantes.

No estipulado.

4.9.7. Periodicidad de la emisión de CRLs y ARLs

La AC del SEPE publica en su repositorio interno listas de certificados revocados, para de esta forma poder validar en todo momento la validez de cada certificado utilizado por las aplicaciones del SEPE. La frecuencia de emisión de estas listas de certificados revocados es la siguiente:

- La AC publica una CRL nueva cada 24 horas como máximo, o en el momento en que se produzca la revocación de un certificado de ciudadano.
- La AC publica una ARL nueva cada 6 horas como máximo, o en el momento en que se produzca la revocación de un certificado de Autoridad de Certificación.

4.9.8. Período de latencia entre la emisión y la publicación de la CRL

No estipulado.

4.9.9. Disponibilidad de un sistema on-line de verificación de certificados

No estipulado.

4.9.10. Requisitos para la verificación on-line de la revocación

No aplica.

4.9.11. Otras formas de divulgación disponibles de la revocación

No estipulado.

4.9.12. Requisitos especiales de renovación de clave comprometida

En caso de compromiso de la clave privada de la AC, se procederá a su revocación inmediata y se informará al resto de las entidades que utilizan los servicios de la AC del SEPE, incluidos suscriptores de certificados y organismos dependientes del SEPE.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

4.9.13. Causas de suspensión

En el ámbito de la AC del SEPE, no se contempla la suspensión (revocación temporal) de certificados de usuario. En todos los casos en los que sea necesario revocar un certificado, éste se revocará de forma permanente.

4.9.14. Quién puede solicitar la petición de suspensión

No aplica.

4.9.15. Procedimiento para la solicitud de suspensión

No aplica.

4.9.16. Límite del período de suspensión

No aplica.

4.10. Servicio de consulta del estado del certificado

SEPE no dispone, como tal, de un servicio de consulta del estado de certificados, lo que se facilita desde la Sede del organismo es un servicio de validación de documentos firmados por el organismo, de tal forma que, como parte de dicha validación, también se comprueba el estado de los certificados.

4.10.1. Características operacionales

No aplica.

4.10.2. Disponibilidad del servicio

No aplica.

4.11. Fin de la suscripción

La suscripción de un certificado expedido por el SEPE puede finalizar en los siguientes casos:

- Revocación del certificado.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

- Vencimiento de la validez del certificado.

4.12. Retención y recuperación de las claves

4.12.1. Políticas y prácticas de recuperación de claves

La clave privada de la AC del SEPE no está sujeta a retención por parte de terceros, sin embargo, está sujeta a copia de seguridad conforme a lo descrito en esta DPC.

Con respecto a los suscriptores, se remite a la Política de Certificación correspondiente a cada tipo de certificado.

4.12.2. Políticas y prácticas de encapsulamiento y recuperación de claves de sesión.

No estipulado.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 5. Uso, operación y controles físicos

En este punto se describen los controles de seguridad no técnicos relativos a la AC del SEPE, en base a los siguientes puntos:

- Seguridad física de las instalaciones.
- Procedimientos de operación implementados.
- Personal encargado de la Infraestructura.

Estos controles se utilizarán para verificar de una forma segura y eficaz la fiabilidad de las funciones relativas al ciclo de vida de los certificados emitidos por la AC del SEPE.

5.1. Controles de seguridad física

5.1.1. Ubicación de las instalaciones

Las instalaciones de la AC del SEPE están protegidas físicamente con las medidas de seguridad necesarias para salvaguardar la información y los equipos utilizados en su actividad.

La localización física de las máquinas y dispositivos concernientes a la AC, es responsabilidad de la Subdirección General de Tecnologías de la Información y Comunicaciones del SEPE, así como cualquier otra medida de seguridad que garantice una protección adecuada contra el acceso físico no autorizado a los equipos y a la información de la Infraestructura.

5.1.2. Acceso físico

El acceso físico a las instalaciones de la AC está protegido por controles de acceso, de modo que sólo el personal autorizado y acreditado puede acceder a las mismas. Estos controles están basados en el chequeo de la tarjeta del empleado por parte de un guardia de seguridad y la confirmación de la aparición del empleado en una lista de personal con acceso autorizado al Centro de Proceso de Datos.

El equipo responsable del Centro de Proceso de Datos y de los accesos físicos al mismo es la Subdirección General de Tecnologías de la Información y Comunicaciones del SEPE.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

5.1.3. Alimentación eléctrica y aire acondicionado

Los equipos informáticos del SEPE están convenientemente protegidos ante fluctuaciones o cortes de suministro eléctrico, que puedan dañarlos o interrumpir el servicio.

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

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

Se realizan controles periódicos de los generadores y fuentes de energía para validar el correcto funcionamiento.

5.1.4. Exposición al Agua

Las instalaciones del SEPE donde se encuentran los equipos están protegidas para evitar las exposiciones al agua de los mismos, mediante detectores de humedad y otros mecanismos de seguridad.

Se realizan controles periódicos de estos elementos.

5.1.5. Prevención y Protección contra Incendios

Las instalaciones del SEPE donde se encuentran los equipos cuentan con las medidas adecuadas de protección contra el fuego, tales como detectores de humo, alarmas, extintores y agua vaporizada en caso de incendio.

Se realizan controles periódicos de todos estos elementos.

5.1.6. Sistema de almacenamiento

El SEPE cuenta con un lugar de almacenamiento, localizado en diferentes Centros de Proceso de Datos, en el que se guarda de manera duplicada toda la información, archivos y copias de seguridad generadas por la Infraestructura de Certificación Electrónica.

El acceso a estos soportes de información está restringido a personal autorizado del SEPE.

5.1.7. Eliminación de los soportes de información

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

La eliminación de soportes, tanto en papel como magnéticos, se realiza mediante mecanismos que garanticen la imposibilidad de recuperación de la información. En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, salvo que puedan volver a utilizarse como medio de soporte, en cuyo caso se elimina la información de manera segura.

En el caso de documentación en papel, la relativa a información confidencial se somete a un tratamiento físico de destrucción.

5.1.8. Salvaguarda fuera de las instalaciones

El SEPE cuenta con un Centro de Recuperación ante Desastres en el que reside una copia de la plataforma de la AC. Este centro consta de medidas de seguridad equivalentes al centro de proceso habitual, y permitirá el restablecimiento del servicio en caso de desastres.

5.2. Controles de procedimientos

El SEPE garantiza que sus sistemas se operan y administran de forma segura, y para este propósito establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

5.2.1. Roles de confianza

De acuerdo a la norma CWA 14167-1, el conjunto de productos que implementan la Autoridad de Certificación del SEPE permite el establecimiento de los siguientes roles para la gestión del sistema:

- **Responsable global de la Infraestructura:** responsable global de la infraestructura corporativa de certificación electrónica del SEPE.
- **Administrador de la Autoridad de Certificación:** responsable de las tareas diarias en la AC, así como de las tareas de configuración y actualización de la misma.
- **Administrador del HSM:** responsable de la gestión de los módulos criptográficos hardware en los que residen las claves privadas y certificados de la AC. El acceso al HSM se realiza mediante usuario y contraseña y llaves hardware propias del HSM.
- **Administrador de sistemas:** responsable del mantenimiento del sistema operativo y hardware sobre la que funciona la Infraestructura de Certificación.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

- **Operador de sistema:** responsable de la gestión del software y hardware de la Infraestructura de Certificación, así como de las copias de seguridad y de respaldo, responsable de gestionar la implementación de las políticas y prácticas de seguridad.

- **Auditor del sistema:** responsable de visualizar los archivos y ficheros de log para tareas de auditoría.

5.2.2. Número de personas requeridas por tarea

Cada una de las tareas de los roles de confianza son realizadas por varias personas, con el fin de reforzar la seguridad e independencia de su actividad. Los usuarios con los roles apropiados acceden al sistema aprovechando la característica de autenticación múltiple de éste.

5.2.3. Identificación y Autenticación para cada Rol

- El **Responsable de Seguridad** define y verifica las políticas, normas y procedimientos de seguridad relacionados con la AC.
- El **Administrador de la AC** se identifica a la AC mediante usuario y contraseña propios de la AC.
- El **Administrador del HSM** se identifica al módulo hardware usuario y contraseña y llaves hardware propias del HSM.
- El **Administrador de sistemas** se identifica a la máquina donde reside la AC con un usuario y contraseña propios del sistema operativo, y que tiene suficientes permisos para realizar operaciones sobre los diferentes elementos de la Infraestructura.
- El **Operador de sistemas** se identifica a la máquina donde reside la AC con su nombre de usuario y su contraseña, generado durante la instalación y activación de la misma.
- El **Auditor de sistema** es el encargado de la consulta de las trazas y logs de los sistemas de la AC, revisando posibles errores en la aplicación de las políticas de seguridad definidas.
- El SEPE autentica e identifica de forma fiable al personal antes de acceder a la realización de sus funciones.

5.2.4. Roles que requieren separación de tareas

La norma CWA 14167-1 establece las siguientes incompatibilidades entre roles:

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

- Incompatibilidad entre los roles administrativos (responsable de seguridad, administrador de sistema y administrador de la AC).
- Incompatibilidad entre los administradores de sistema y el administrador del HSM.
- Incompatibilidad entre el administrador de la AC y el administrador del HSM.
- Incompatibilidad entre el auditor y cualquiera de los otros roles.

5.3. Controles de seguridad del personal

5.3.1. Requisitos relativos a la cualificación y experiencia profesionales

El personal que presta sus servicios en el ámbito de la Autoridad de Certificación del SEPE deberá poseer el conocimiento, experiencia y formación suficientes, para el correcto cometido de las funciones asignadas.

Para ello, el SEPE llevará a cabo los procesos de selección de personal que estime precisos con objeto de que el perfil profesional del empleado (tanto interno como externo) se adecue lo más posible a las características propias de las tareas a desarrollar.

5.3.2. Requisitos del personal de los roles de confianza

El SEPE posee unas prácticas de personal que garantizan la aptitud del personal de confianza, así como unos procedimientos de control adecuados para el cumplimiento de los derechos y obligaciones establecidos en la presente DPC.

5.3.3. Procedimientos para la verificación de antecedentes

Las prácticas de selección y reclutamiento de personal son las ya definidas por el SEPE. Estas prácticas aseguran los requisitos de experiencia, cualificación e historial precisos para cada puesto, sea de un rol de confianza o no.

5.3.4. Requisitos de formación

El SEPE provee al personal relacionado con la explotación de la Autoridad de Certificación de toda la información y documentación necesaria sobre los procedimientos operativos relativos a la misma.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

5.3.5. Períodos y procedimientos de formación

Según los procedimientos establecidos por SEPE.

5.3.6. Frecuencia y serie de rotaciones de trabajo entre varios roles

No estipulado.

5.3.7. Sanciones

Las prácticas internas del personal del SEPE definen el procedimiento sancionador para los funcionarios que incumplen las mismas, especificando las sanciones por efectuar una acción no autorizada, el uso no autorizado de la Autoridad de Certificación o el uso no autorizado de los sistemas.

En cualquier caso, si el SEPE sospecha que algún empleado está efectuando una acción no autorizada, automáticamente suspenderá su permiso de acceso a todos los sistemas de información del SEPE.

5.3.8. Requisitos para la contratación de personal

El SEPE contrata personal cualificado para las tareas relacionadas con la AC.

Los perfiles de empleados externos asociados con estas tareas se detallan en los pliegos de contratación de las empresas.

5.3.9. Documentación suministrada al personal

El SEPE proporciona a sus empleados toda la documentación necesaria para el correcto desempeño de sus tareas, incluyendo la necesaria para las tareas descritas en esta DPC y la Normativa de Seguridad del SEPE.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de acontecimientos registrados

El SEPE guarda registro de los eventos relacionados con la seguridad de la AC.

5.4.2. Frecuencia de tratamiento de registros de auditoría

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye: verificación de que éstos no han sido manipulados, breve inspección de todas las entradas de registro e investigación más profunda de cualquier alerta o irregularidad en los registros.

Las acciones realizadas a partir de la revisión de auditoría también son documentadas.

5.4.3. Periodo de conservación de registros de auditoría

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

5.4.4. Protección de los registros de auditoría

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

Los registros software de la AC están protegidos por técnicas criptográficas, de modo que nadie, excepto la aplicación de visualización de eventos, con un adecuado control de acceso, puede acceder a ellos.

5.4.5. Procedimientos de salvaguarda

Se realizan copias de seguridad periódicas de los registros de auditoría generados por el la AC del SEPE.

5.4.6. Sistema de recogida de datos de auditoría

El sistema de recogida de datos de auditoría es de carácter manual y automático y es interno al SEPE. Los registros de seguridad física también son parte de la colección de auditoría.

5.4.7. Notificación de la causa del evento

No estipulado.

5.4.8. Análisis de vulnerabilidades

Los eventos de auditoría se guardan, entre otros motivos, para monitorizar las vulnerabilidades del sistema.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

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

5.5. Archivo de informaciones

La AC del SEPE conserva toda la información relevante sobre las operaciones realizadas con los certificados durante los periodos de tiempo establecidos, manteniendo un registro de eventos.

5.5.1. Tipos de eventos registrados

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

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

- Datos relacionados con el procedimiento de registro y solicitud de certificados.
- Declaración de Prácticas de Certificación.
- Políticas de Certificación.

El SEPE guarda todos los eventos que tiene lugar durante el ciclo de vida de un certificado, incluyendo la emisión, uso, revocación, suspensión y renovación de éste y su par de claves asociadas.

5.5.2. Periodo de conservación de registros

Toda la información y documentación sobre el ciclo de vida de los certificados emitidos por la AC se mantiene por un período de 15 años.

5.5.3. Protección del archivo

El SEPE mantiene la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.

Además, archiva los datos indicados anteriormente de forma completa y confidencial, y mantiene la privacidad de los datos de registro del suscriptor.

5.5.4. Procedimientos de copia de seguridad

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

El procedimiento de salvaguarda de la AC conlleva la realización de una copia de seguridad de los siguientes conjuntos de datos:

- Software-Hardware de base:
    - Datos de configuración estática y dinámica de la AC.
    - Información contenida en el HSM (claves privadas y certificados).
- Datos de Producción:
    - Backup completo de datos, generado automáticamente por el sistema, que incluye:
        - Datos almacenados en la Base de Datos, incluidos perfiles de acceso.
        - Datos almacenados en el Directorio LDAP relativos a certificados de usuarios, objetos, entradas o atributos.
        - Ficheros con la Política de Seguridad implementada en el Sistema.
        - Ficheros de configuración.
        - Ficheros de registro.
    - Backup incremental de datos, generado automáticamente por el sistema, que incluye:
        - Cambios en la Base de Datos desde el último backup completo o incremental
        - Cambios en el Directorio desde el último backup completo o incremental.

Esta copia de seguridad se copia de forma automática al Centro de Respaldo.

5.5.5. Requisitos para validación cronológica de registros

Los sistemas de información empleados por el SEPE garantizan el registro del tiempo en los que se realizan. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. Todos los servidores que conforman la Infraestructura de Certificación Electrónica del SEPE están sincronizados en fecha y

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

hora. Las fuentes de tiempos utilizadas, basadas en el protocolo NTP (*Network Time Protocol*), se sincronizan utilizando como referencia la del Real Instituto y Observatorio de la Armada.

5.5.6. Localización del sistema de archivo

El SEPE tiene un sistema de mantenimiento de datos de archivo en sus propias instalaciones.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Solamente personas autorizadas por el SEPE tendrán acceso a los datos de archivo almacenado en las mismas instalaciones del SEPE.

5.6. Renovación de claves y certificados

La renovación del certificado de la AC del SEPE se realizará de forma manual y con la antelación necesaria a la fecha de expiración del mismo.

La renovación de los certificados de entidades finales se realizará conforme a lo especificado en la correspondiente Política de Certificación.

5.7. Compromiso de claves y recuperación ante desastres

5.7.1. Procedimiento de gestión de incidencias y compromisos

El SEPE establece los procedimientos que definen las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental, que inutilice o degrade los recursos y los servicios de certificación prestados por SEPE.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un acontecimiento de corrupción de recursos, aplicaciones o datos, SEPE procederá a detener los servicios de la AC hasta que se puede verificar la seguridad del entorno, si es necesario sustituyendo los componentes afectados por otros cuya integridad ha sido debidamente verificada.

De forma simultánea, se realizará una auditoría para identificar la causa de la alteración y asegurar su no reproducción.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

5.7.3. Compromiso de la clave privada de la Autoridad de Certificación

El SEPE considera el compromiso o la sospecha de compromiso de la clave privada de la AC como un desastre.

En caso de verse comprometida la seguridad de la clave privada de la AC, el SEPE procederá a realizar las siguientes acciones:

- Revocar el certificado de la AC actual, de tal forma que los certificados emitidos por esa AC dejen de tener validez.
- El SEPE informará a todos los titulares de certificados que todos los certificados emitidos por esa AC ya no son válidos.
- Generar una nueva AC con una clave de firma y certificados nuevos.
- Tan pronto como sea posible se procederá al restablecimiento del servicio.

5.7.4. Desastre sobre las instalaciones

El SEPE desarrolla, mantiene, prueba y, dado el caso, ejecuta un plan de emergencia en el caso de desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, que indique cómo se restauran los servicios de los Sistemas de Información, y en concreto, como se restaura la AC, pasando el Centro de Respaldo a ofrecer el servicio.

5.7.5. Finalización del servicio

El SEPE podrá finalizar el servicio ofrecido por su AC en cualquier momento, notificando previamente de dicho cambio a sus suscriptores.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 6. Controles Técnicos de Seguridad

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves de la AC del SEPE se genera y almacena en un módulo de hardware criptográfico seguro (HSM), que cumple los requisitos establecidos en el estándar FIPS 140-2 Nivel 3.

Las claves y certificados de entidades se emiten según lo dispuesto en la Política de Certificación correspondiente al tipo de certificado.

6.1.2. Entrega del par de claves al titular

El envío de la clave privada al titular se realizará de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

6.1.3. Entrega de la clave pública al emisor del certificado

La entrega de la clave pública al titular se realizará de acuerdo con lo dispuesto en la Política de Certificación de cada tipo de certificado.

6.1.4. Entrega de la clave pública de la AC

El certificado de la AC se publica en los repositorios internos del SEPE.

6.1.5. Longitud de las claves

Las claves de la AC del SEPE son de 2048 bits.

La longitud de las claves de los suscriptores de certificados, se especifica en la correspondiente Política de Certificación.

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

Los parámetros de clave pública son generados conforme a la norma PKCS#1. El algoritmo usado para la generación de las claves es RSA.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

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

La extensión "*keyUsage*" de los certificados indica el uso para el que deben ser utilizados según se recomienda en el RFC-3280, y debe establecerse como extensión crítica.

El uso concreto para cada tipo de certificado viene determinado en la correspondiente Política de Certificación.

6.2. Protección de la clave privada y características del módulo criptográfico

6.2.1. Normas y medidas de seguridad del módulo criptográfico

La puesta en marcha de la AC del SEPE conlleva la generación de la clave privada de la misma en un módulo hardware seguro (HSM), sujeto al estándar FIPS-140-2 nivel 3.

6.2.2. Control multipersona (K de N) de la clave privada

La clave privada de la AC se encuentra bajo control multipersona. Ésta se activa mediante la inicialización del software de AC por medio de una combinación de operadores de la AC, y operadores del módulo hardware seguro.

La clave privada de los certificados están bajo el control del titular del mismo, y su protección viene especificada en la correspondiente Política de Certificación.

6.2.3. Custodia de la clave privada

La clave privada de la AC se encuentra almacenada y protegida en el HSM, y nunca sale del mismo.

6.2.4. Copia de seguridad de la clave privada

Se realizan copias de seguridad de la clave privada de la AC durante el proceso de generación de las mismas.

Estas copias se realizan a efectos de continuidad de negocio para la recuperación ante desastres. Las copias de seguridad, tienen el mismo nivel de seguridad que la clave original. Las copias de la clave se guardan en una localización física diferente a aquella donde está ubicada la AC.

El método de copia de seguridad de las claves privadas de entidades finales viene especificado en la correspondiente Política de Certificación.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

6.2.5. Transferencia de la clave privada

La transferencia de la clave privada de la AC del SEPE sólo se puede hacer entre módulos hardware criptográfico (HSM) y requiere de la intervención de un administrador del sistema y un administrador de HSM.

La transferencia de las claves privadas asociadas a los certificados de entidades finales se describe en las Políticas de Certificación asociadas a cada tipo de certificado.

6.2.6. Almacenamiento de la clave privada

La clave privada de la AC se almacena y protege en el HSM vinculado a la AC en el momento de la activación de la misma.

Las claves privadas de entidades finales se almacenan conforme viene descrito en la correspondiente Política de Certificación.

6.2.7. Método de activación de la clave privada

La clave privada de la AC del SEPE se activa mediante la inicialización del software de AC por medio de la combinación mínima de dos operadores de la AC correspondiente.

La activación de las clave privadas y de los certificados de entidades se estipula en la Política de Certificación correspondiente.

6.2.8. Método de desactivación de la clave privada

La clave privada de la AC no se desactiva en ningún momento.

Para las claves privadas de entidades finales se remite a la correspondiente Política de Certificación.

6.2.9. Proceso para destrucción de la clave privada

Cuando sea necesario, el SEPE destruirá la clave privada de la AC y su copia de seguridad para garantizar que no se mantiene información residual que se pueda utilizar para reconstruir la clave privada.

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

El método de destrucción de las claves privadas de entidades finales se describe en la correspondiente Política de Certificación.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

6.3. Otros aspectos de la gestión de claves

6.3.1. Archivo de la clave pública

La AC del SEPE archiva sus claves públicas, de acuerdo con lo establecido en este documento.

6.3.2. Periodos de validez del certificado y las claves

El periodo de utilización de las claves está determinado por el periodo de validez del certificado de modo que después de la expiración del certificado, las claves no podrán utilizarse, produciéndose el cese permanente de su funcionamiento para el uso para el que fueron generadas.

El tiempo de vida de la clave privada de la AC está configurado a 25 años.

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

Los períodos de validez para los diferentes tipos de certificado emitidos por la AC del SEPE se especifican en la correspondiente Política de Certificación.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

Para la activación de las claves privadas de la AC, es necesaria la intervención mínima del administrador de sistemas, operadores de la AC y administradores del HSM. Éste es el único método de activación de dicha clave privada.

En el caso de las claves de los certificados emitidos por la AC, la generación de los datos de activación se indica en la correspondiente Política de Certificación.

6.4.2. Protección de los datos de activación

Esta información se especifica en la correspondiente Política de Certificación asociada al tipo de certificado concreto.

6.4.3. Otros aspectos de los datos de activación

No estipulado.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

6.5. Medidas de seguridad

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

6.5.1. Requisitos técnicos específicos

El SEPE garantiza que los elementos que acompañan al sistema de certificación de clave pública, están protegidos contra accesos no autorizados.

Adicionalmente el SEPE limita el acceso a estos sistemas únicamente a individuos que desempeñan un papel de confianza y motivos válidos para dicho acceso.

El acceso directo a la base de datos que apoya las operaciones de AC se limita a las personas con función de confianza, tal como se describe en esta DPC.

6.5.2. Evaluación del nivel de seguridad

Los distintos sistemas y productos utilizados por el SEPE son fiables y están protegidos contra modificaciones. El SEPE evalúa continuamente los sistemas en busca de vulnerabilidades o fallos, y realiza auditorías para garantizar la seguridad de todos los sistemas relacionados con el ciclo de vida de los certificados.

6.6. Medidas técnicas de seguridad del ciclo de vida

6.6.1. Medidas de desarrollo de sistemas

No estipulado.

6.6.2. Medidas para la gestión de seguridad

No estipulado.

6.6.3. Medidas de seguridad del ciclo de vida

No estipulado.

6.7. Controles de seguridad de red

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

La infraestructura de red utilizada por el sistema está dotada de todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro (por ejemplo, utilización de cortafuegos o intercambio de datos cifrados entre redes). Esta red también es auditada periódicamente.

6.8. Fuentes de tiempo

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

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 7. Perfiles de certificados y CRL

7.1. Perfil del certificado de la AC

El certificado de la AC contiene los siguientes campos y extensiones:

Atributo	Valor	Tipo
Versión	V3	Campo v1
Número de serie	No secuencial	Campo v1
Algoritmo de firma	SHA1withRSAEncryption	Campo v1
Emisor	OU=AC SPEE, O=SPEE, C=ES	Campo v1
Válido desde	lunes, 19 de octubre de 2009 20:24:59	Campo v1
Válido hasta	jueves, 19 de octubre de 2034 20:54:59	Campo v1
Asunto	OU=AC SPEE, O=SPEE, C=ES	Campo v1
Clave pública	Algoritmo: RSA Encryption Longitud Clave: 2048 Bits	Campo v1
Subject Key Identifier	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	Extensión
Puntos de distribución de la CRL	CN=CRL1, OU=AC SPEE, O=SPEEE, C=ES	Extensión
Uso de la clave	Firma de Certificados Firma de CRLs sin Conexión Firma de CRLs	Extensión crítica
Restricciones básicas	Entidad Emisora de Certificados (CA)	Extensión crítica
Algoritmo de identificación	SHA1	Propiedad
Firma digital	No disponible	Propiedad

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Nombre descriptivo	Comentario	Propiedad

7.2. Perfil de CRL

A continuación se recogen los perfiles de los dos tipos de listas de certificados revocados que emite la AC del SEPE:

7.2.1. Lista de certificados revocados (CRL)

Atributo	Atributo	Atributo
Versión	V3	Campo v1
Número de serie	No secuencial	Campo v1
Algoritmo de firma.	SHA1withRSAEncryption	Campo v1
Emisor	OU=AC SPEE, O=SPEE, C= ES	Campo v1
Válidez	24 horas	Campo v1

7.2.2. Lista de autoridades revocadas (ARL)

Atributo	Atributo	Atributo
Versión	V3	Campo v1
Número de serie	No secuencial	Campo v1
Algoritmo de firma.	SHA1withRSAEncryption	Campo v1
Emisor	OU=AC SPEE, O=SPEE, C=ES	Campo v1
Validez	6 horas	Campo v1

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 8. Auditorías de cumplimiento y otros controles

8.1.1. Frecuencia y motivos de la auditoría

Se llevará a cabo regularmente una auditoría sobre la AC del SEPE para garantizar la adecuación de su funcionamiento y operativa con la normativa estipulada en esta DPC.

Además, el SEPE podrá realizar auditorías bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.1.2. Identificación/cualificación del auditor

La realización de las auditorías podrá ser encargada a empresas auditoras externas o al Departamento de Auditoría Interna del SEPE en función de la disponibilidad de personal cualificado en los aspectos concretos a auditar.

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

- Experiencia profesional y conocimientos en infraestructuras de clave pública, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo del SEPE.

8.1.3. Relación entre el auditor y la Autoridad de Certificación

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

8.1.4. Ámbito de la auditoría

La auditoría se realizará sobre estos elementos:

- AC y elementos relacionados.
- Sistemas de información.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

- Documentación relacionada.
- Controles de acceso físicos y lógicos.

8.1.5. Acciones a emprender como resultado de la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. El responsable de seguridad de la AC del SEPE deberá realizar las siguientes acciones:

- Tomar de inmediato las medidas para su corrección.
- Definir, en base a las causas identificadas, medidas correctivas, los responsables y los plazos, establecer y proporcionar los recursos necesarios para la ejecución de las acciones.

En el caso de observarse deficiencias graves, el SEPE, en calidad de prestador de servicios de certificación, podrá adoptar, entre otras, las siguientes decisiones:

- Suspensión temporal de las operaciones hasta que las deficiencias sean solventadas.
- Suspensión o revocación del certificado raíz de la AC.
- Cambios en el personal implicado de administrar la AC.

8.1.6. Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría a la Subdirección General de Tecnologías de la Información y Comunicaciones del SEPE.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

Capítulo 9. Otras cuestiones legales y de actividad

9.1. Tarifas

9.1.1. Tarifas por emisión y renovación de certificados

No estipulado.

9.1.2. Tarifas para el acceso al certificado

No estipulado.

9.1.3. Tarifas para acceso a la información del estado de revocación del certificado

No estipulado.

9.1.4. Tarifas para otros servicios

No estipulado.

9.1.5. Politica de reembolso

No estipulado.

9.2. Responsabilidad Financiera

9.2.1. Seguro de cobertura

No estipulado.

9.2.2. Otros recursos

No estipulado.

9.2.3. Seguro de cobertura o garantia de cobertura para usuarios

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

No estipulado.

9.3. Confidencialidad de la información procesada

9.3.1. Ámbito de confidencialidad de la información

Toda la información dentro de la AC del SEPE es confidencial, salvo la información mencionada en las secciones 9.3.2 y 9.4.3.

9.3.2. Información no confidencial

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

- La contenida en la presente Declaración de Prácticas de Certificación.
- Las Políticas de Certificación de los certificados emitidos por la AC del SEPE.

9.3.3. Responsabilidad de protección de la confidencialidad de la información

Todo el personal encargado de la administración, operación y supervisión de la AC del SEPE mantiene la confidencialidad sobre la información disponible, en virtud del ejercicio de sus funciones. Esta obligación se extiende a personal interno y externo que colabora en virtud de las obligaciones contractuales establecidas con el SEPE.

9.4. Privacidad de datos personales

9.4.1. Medidas para garantizar la privacidad

De acuerdo con la legislación española de protección de datos de carácter personal.

9.4.2. Información considerada como privada

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

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

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

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

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

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

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

9.4.3. Información no considerada como privada

Es considerada no confidencial la siguiente información:

- Certificados de clave pública.
- Listas de certificados revocados (CRLs).
- Listas de autoridades revocadas (ARLs).
- Los usos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad del mismo.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

9.4.4. Responsabilidad de la protección de los datos de carácter personal

De acuerdo con la legislación española de Protección de Datos de Carácter Personal.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

9.4.5. Comunicación y consentimiento para usar datos de carácter personal

De acuerdo con la legislación española de Protección de Datos de Carácter Personal.

9.4.6. Revelación en el marco de un proceso judicial

De acuerdo con la legislación española de Protección de Datos de Carácter Personal.

9.4.7. Otras circunstancias de publicación de información

De acuerdo con la legislación española de Protección de Datos de Carácter Personal.

9.5. Derechos de propiedad Intelectual

El Servicio Público de Empleo Estatal (SEPE) es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Declaración de Prácticas de Certificación.

Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva del Servicio Público de Empleo Estatal sin la autorización expresa por su parte.

9.6. Obligaciones y responsabilidad civil

9.6.1. Autoridad de Certificación

Los servicios prestados por la AC del SEPE en el contexto de esta DPC son los servicios de emisión y revocación de certificados, y emisión de listas de revocación de acuerdo con esta DPC.

El SEPE, como prestador de servicios de certificación:

1° Actuará relacionando una determinada clave pública con su titular a través de la emisión de los certificados, de conformidad con los términos de la DPC.

2° Prestará servicios en el contexto de la DPC con los servicios de emisión, renovación y revocación de los certificados.

3° Comunicará los cambios de la DPC de acuerdo con lo establecido en el propio documento.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

4º Emitirá certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores en la entrada de datos.

5º Revocará los certificados en los términos recogidos en la DPC.

6º Pondrá a disposición de los ciudadanos los certificados correspondientes a la AC del SEPE.

7º Protegerá la clave privada de la AC del SEPE.

8º Utilizará sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

9º Almacenará de forma fiable y segura los datos de creación de firma, clave privada, de los titulares de certificados de firma garantizando que sólo el titular puede acceder al mismo.

10º Responderá por los daños y perjuicios que se causen a cualquier ciudadano en el ejercicio de su actividad cuando incumpla las obligaciones que les impone la Ley 59/2003, de 19 de Diciembre, de Firma Electrónica.

11º No será responsable del contenido de aquellos documentos firmados electrónicamente por los ciudadanos con las claves generadas por esta AC.

12º Conservar registrada toda la información y documentación relativa a los certificados de identidad pública durante un mínimo de quince años.

13º Colaborar con los procesos de auditoría que se realicen sobre la Infraestructura de Certificación.

14º Operar de acuerdo con la legislación aplicable. En concreto con:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.

15º En el caso de cesar en su actividad, deberá comunicarlo con una antelación mínima de dos meses, a los titulares de los certificados por ella emitidos.

9.6.2. Obligaciones y garantías de la Autoridad de Registro

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

No estipulado.

9.6.3. Obligaciones y garantías del titular

No estipulado.

9.6.4. Obligaciones y garantías de los suscriptores

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

1° Suministrar a las Autoridades de Registro (oficinas del SEPE) información exacta, completa y veraz en relación a los datos que estas les soliciten para realizar el proceso de registro.

2° Conocer y aceptar las condiciones de utilización de los certificados.

3° Utilizar de forma correcta el certificado electrónico y sus claves.

4° Comunicar al SEPE, a través de los mecanismos que se habilitan a tal efecto, cualquier mal funcionamiento del certificado.

5° Proteger su contraseña de acceso al Portal de Sede Electrónica, tomando las precauciones razonables para evitar su pérdida, revelación o uso no autorizado.

6° Cumplir las obligaciones que se establecen para el usuario en la DPC y en el artículo 23.1 de la Ley de Firma Electrónica.

7° El ciudadano asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

8° Así mismo, el ciudadano se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al ciudadano.

9.6.5. Obligaciones y garantías de Terceros aceptantes

Es obligación de los terceros que acepten y confíen en los certificados emitidos por la Autoridad de Certificación del SEPE:

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

1° Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y en esta DPC.

2° Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.

3° Asumir su responsabilidad en la comprobación de la validez y del estado de revocación de los certificados en que confía.

4° Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.

9.7. Renuncia de garantías

No estipulado.

9.8. Limitaciones y obligaciones

No estipulado.

9.9. Indemnizaciones

No estipulado.

9.10. Duración y cese de actividad

9.10.1. Duración

La Declaración de Prácticas de Certificación y las Políticas de Certificación entrarán en vigor en el momento de su publicación en el portal del SEPE (**http://sede.sepe.gob.es/dpc**), y permanecerán vigentes hasta su sustitución por una nueva versión de las mismas.

9.10.2. Finalización de la Declaración de Prácticas de Certificación

La Declaración de Prácticas de Certificación y las Políticas de Certificación serán sustituidas por las nuevas versiones de estos documentos aprobadas por el SEPE.

9.10.3. Consecuencias de la finalización de la actividad y la supervivencia

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

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

9.11. Notificaciones individuales y comunicaciones con los participantes

No estipulado.

9.12. Procedimientos de cambios en las especificaciones

9.12.1. Procedimiento para los cambios

La autoridad con atribuciones para realizar y aprobar cambios sobre esta DPC es la Subdirección General de Tecnologías de la Información y Comunicaciones del SEPE.

9.12.2. Periodo y procedimiento de notificación

Los cambios en la DPC se comunicarán en la Sede Electrónica del SEPE a fin divulgar la nueva versión de la misma.

9.12.3. Circunstancias en las que el OID debe ser cambiado

No estipulado.

9.13. Disposiciones para la resolución de conflictos

Las partes interesadas se reunirán para resolver cualquier conflicto que pueda surgir en relación con esta Declaración de Prácticas de Certificación (DPC).

9.14. Normativa Aplicable

Las operaciones y funcionamiento de la AC del SEPE, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

- Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley 59/2003, de 19 de Diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de Junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

9.15. Cumplimiento de la normativa aplicable

Es responsabilidad de todos los intervinientes en el sistema de certificación de clave pública del SEPE velar por el cumplimiento de la legislación aplicable recogida en el apartado anterior.

9.16. Cláusulas diversas

No estipulado.

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81

C/ Condesa de Venadito 9
28027 MADRID
TEL: 91 585 98 88
FAX: 91 377 58 81