D3.3.7 SESCAM - Declaración de Practicas de Certificación

CONTENIDO

1 INTRODUCCION

El SESCAM pretende ser una organización de servicios sanitarios públicos moderna y de vanguardia, que se caracterice por la innovación y la calidad del servicio global (medicina, enfermería, servicios auxiliares, hostelería), por la precisión en el diagnóstico y en el tratamiento, su seguridad, cercanía y agilidad. Sus servicios deben procurar el confort de los usuarios, prestando una atención personalizada que garantice la confidencialidad. Debe posibilitar tanto la participación social como la de los profesionales, facilitando la atención y el trato adecuados a los proveedores. Asimismo, en sus actuaciones debe primar la eficiencia en el uso del dinero público.

En este sentido la misión del SESCAM consiste en ofrecer una buena atención sanitaria a toda la población de Castilla-La Mancha, y a todos los usuarios de los servicios, ofreciendo un lugar de trabajo estable, confortable y estimulante a sus trabajadores.

La Atención Sanitaria, el contenido esencial del trabajo del SESCAM, es un servicio complejo (diagnóstico, pronóstico, tratamiento), que requiere profesionales bien formados, medios suficientes, y una adecuada organización.

En tal sentido, uno de los objetivos del SESCAM es dotar a los servicios y profesionales sanitarios de las herramientas adecuadas para agilizar y facilitar su trabajo y por ende el servicio prestado a los ciudadanos de Castilla la Mancha., por lo que la opción a favor de un modelo de certificación que se encuentra expresamente inspirada por el artículo 4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que contempla la posibilidad de que la prestación de los servicios de certificación pueda efectuarse por las Administraciones o los organismos o sociedades de ellas dependientes.

El modelo de certificación referido ajusta su ámbito de actuación inicialmente al soporte necesario para la implantación de medidas de seguridad y firma electrónica avanzada en el entorno operativo del SESCAM y las entidades dependientes de éste, como medida inicial para agilizar los procesos organizativos de la institución.

Si bien, el modelo de certificación inicial no recoge la prestación de servicios de certificación pública a los ciudadanos de Castilla la Mancha en el ámbito de las relaciones de éstos con los servicios sanitarios ofrecidos en la región, el sistema recogido en esta Declaración de Practicas de Certificación ha sido expresamente preparado para poder ser utilizado en el futuro, sin perjuicio de los servicios que se prestan en la actualidad.

1.1 Presentación

El presente documento constituye la Declaración de Practicas de Certificación, en adelante DPC, del SESCAM.

La presente DPC expone las normas y condiciones generales de los servicios de certificación que presta el SESCAM cuando actúa como Autoridad de Certificación digital incluyendo la solicitud, identificación, emisión, aceptación, gestión, uso y revocación de los certificados.

No están incluidas en esta DPC las Políticas de Certificación específicas para cada tipo de certificado, las cuales pueden encontrarse en el documento ***"D3.2.2 SESCAM– Políticas de Certificación".***

1.1.1 Clases de certificados

La infraestructura de clave pública del SESCAM emite y gestiona diferentes clases y tipos de certificados según el uso que se pretende dar a las claves asociadas al mismo, y el tipo de usuario de las mismas. Bajo estas premisas SESCAM ha considerado oportuno dividir el conjunto de clases de certificados según:

- Clase 1 – Correspondiente a la propia autoridad de certificación raíz.
- Clase 2 – Correspondiente a los certificados propios a la gestión de la infraestructura de clave pública que es gobernada por esta declaración.
- Clase 3 – Certificados de Empleados del Sescam.
- Clase 4 – Certificados de Dispositivos.
- Clase 5 – Certificados de firma de código

Bajo cada una de estas clases se emiten y gestionan diversos tipos de certificado dependiendo del uso al que los mismos están destinados. El conjunto global de certificados regidos por esta Declaración de Practicas es el siguiente:

Clase	Nombre Certificado	Descripción
Clase 1	Política de CA Raíz	Certificado de la Autoridad de Certificación Raíz. El certificado emitido bajo esta política es autofirmado y será utilizado para la firma de certificados de Autoridad de Certificación (CA) y de las listas de revocación (ARLs) correspondientes.
Clase 2	Política de CA Subordinada	Certificado de la Autoridad de Certificación Subordinada.

		Los certificados emitidos bajo esta política están firmados por la Autoridad de Certificación Raíz y serán utilizados para la firma de certificados de Autoridad de Registro (AR), de Entidad Final (EF) y de las listas de revocación (LCRs) correspondientes.
Clase 2	Política de AR	Certificado de la Autoridad de Registro. Los certificados emitidos bajo esta política están firmados por la Autoridad de Certificación Subordinada y serán utilizados para la firma de lotes de peticiones. Este tipo de certificados deberá ser dado de alta en la Autoridad de Certificación Subordinada como AR reconocida.
Clase 2	Política GESUSER	Estos certificados corresponden a los utilizados por los componentes asociados a las Autoridades de Registro. Serán utilizados para autenticarse frente a la Autoridad de Registro y para firmar los lotes de peticiones. A priori, el único componente de registro autorizado para el uso de este tipo de certificado corresponde a la identidad representada por la aplicación GESUSER.
Clase 3	Política de EF de Empleado para Autenticación.	Certificado de Autenticación para empleados del SESCAM emitido por la Autoridad de Certificación y cuyo propósito es el de identificar al usuario exclusivamente. Este certificado no vincula al usuario en ninguna forma y es exclusivamente utilizado para el establecimiento de canales privados y confidenciales con los posibles prestadores de servicio y/o aplicaciones del SESCAM como por ejemplo pueden ser los servidores WEB o el acceso al Dominio de Windows 2000.
Clase 3	Política de EF de Empleado para No-Repudio.	Certificado de No-Repudio para empleados del SESCAM emitido por la Autoridad de Certificación y cuyo propósito es el de permitir al funcionario firmar tramites y documentos. Este certificado es un certificado cualificado según ETSI y la RFC3739 y permite sustituir la firma manuscrita por la electrónica en las relaciones del usuario con terceros

Clase 3	Política de EF de Empleado para Cifrado.	Certificado de Cifrado para empleados del SESCAM emitido por la Autoridad de Certificación y cuyo único propósito es garantizar la confidencialidad de la información. Inicialmente este certificado será sólo utilizado para el cifrado de correos electrónicos, si bien su uso podrá extenderse al cifrado de documentos o ficheros.
Clase 4	Política de EF Dispositivo Físico de Servidor WEB	Los certificados emitidos bajo esta política estarán destinados a su uso en los servidores WEB del SESCAM y entidades asociadas. Los certificados emitidos bajo esta política se utilizarán para garantizar el origen de las comunicaciones y establecer canales seguros SSL/TLS con los navegadores cliente que accedan a los mismos.
Clase 4	Política de EF Controlador de dominio W2K	Estos certificados son utilizados por los controladores de dominio de Windows del SESCAM y entidades asociadas, el certificado es emitido por la Autoridad de Certificación. El ámbito de uso de estos certificados esta orientado al establecimiento de conexiones autenticadas entre los diferentes elementos de la red.
Clase 5	Política de Firma de Código	Certificados emitidos por la autoridad de certificación subordinada cuyo objeto es garantizar la autenticidad e integridad de las diferentes aplicaciones software desarrolladas por el SESCAM.

1.2 Identificación

La presente Declaración de Practicas de Certificación se identifica con el nombre "DPC del SESCAM Versión 1" , habiéndole sido asignado el OID = 1.3.6.1.4..21835.1.1. La misma puede ser públicamente accedida en la siguiente dirección de Internet:

http://sescam.jccm.es/pki/dpc/dpc.html.

Con el objeto de identificar de forma individual, cada clase y tipo de certificado emitido por el SESCAM de acuerdo con la presente Declaración de Prácticas de Certificación, se asigna un identificador de objeto (OID) a cada uno, que aparecerá en la extensión correspondiente de cada certificado emitido.

Clase de Certificado	Politica de Certificado	OID Asignado
Clase 1 – Correspondiente a la propia autoridad de certificación raíz.	Política de CA Raíz	1.3.6.1.4.1. 21835.1.1.**1**
Clase 2 – Correspondiente a los certificados propios a la gestión de la infraestructura de clave pública que es gobernada por esta declaración.	Política de CA Subordinada	1.3.6.1.4.1.21835.1.1.**2**
	Política de AR	1.3.6.1.4.1.21835.1.1.**2**.1
	Política para GESUSER	1.3.6.1.4.1.21835.1.1.**2**.1.1
Clase 3 – Certificados de Empleados del Sescam.	Política de EF de Empleado para Autenticación.	1.3.6.1.4.1.21835.1.1.**3**.1
	Política de EF de Empleado para No-Repudio.	1.3.6.1.4.1.21835.1.1.**3**.2
	Política de EF de Empleado para Cifrado.	1.3.6.1.4.1.21835.1.1.**3**.3
Clase 4 – Certificados de Dispositivos.	Política de EF Dispositivo Físico de Servidor WEB	1.3.6.1.4.1.21835.1.1.**4**.1
	Política de EF Controlador de dominio W2K	1.3.6.1.4.1.21835.1.1.**4**.2
Clase 5 – Certificados de Firma de Código	Política de Firma de Código	1.3.6.1.4.1.21835.1.1.**5**

Aquellos certificados emitidos como reconocidos incorporan además el identificador de política definido por el Instituto Europeo de Normas de Telecomunicación ETSI TS 101 862 sobre perfiles de certificados reconocidos, estos corresponden en principio únicamente a los certificados de clase 3 emitidos bajo la política "Política de EF de Empleado para No-Repudio".

1.3 Comunidad de usuarios y aplicabilidad

Los servicios prestados por la PKI del SESCAM son apropiados para aquellas situaciones en donde las partes exigen garantías de autenticidad, no repudio y confidencialidad.

El propósito de la Infraestructura de PKI que será emplazada en las dependencias del SESCAM ofrece solución inmediata a los siguientes aspectos:

- ***Autenticación de Usuarios***, mediante el uso de tarjetas inteligentes frente a los sistemas del SESCAM, para lo cual deberá implantarse una solución de "logon" único frente a los mismos.
- ***Correo Electrónico***, se requiere que los correos intercambiados entre los usuarios del SESCAM puedan ser firmados y cifrados.
- **Firma electrónica de Documentos**, para ello el SESCAM desarrolla las acciones correspondientes para que las aplicaciones existentes dentro de su organización puedan hacer un adecuado uso de la misma.

El sistema de certificación del SESCAM se compone de los siguientes roles:

- Autoridades de Certificación
- Autoridades de Registro
- Autoridad de Recuperación de claves
- Entidades finales

1.3.1 Autoridad de Certificación

El SESCAM actúa como Autoridad de Certificación (AC) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de Certificados digitales.

La jerarquía de la infraestructura de clave pública del SESCAM se compone de dos niveles representados por una Autoridad de Certificación Raíz que emitirá y gestionará certificados de la entidades de certificación secundarias o de producción, las cuales serán responsables de la emisión de certificados para entidades finales y para sus propias Autoridades de Registro además de las correspondientes Listas de Revocación. En la actualidad el SESCAM opera únicamente una Autoridad de Certificación de Producción responsable de la emisión de los certificados de clase 3, clase 4 y clase 5.

1.3.1.1 Autoridad de Recuperación de claves

La Autoridad de Recuperación de claves del SESCAM garantizará la salvaguardia y confidencialidad de las claves de cifrado de los usuarios.

1.3.2 Autoridad de Registro

La Autoridad de Certificación (AC) del SESCAM podrá valerse de una o varias Autoridades de Registro (AR). Estas autoridades de Registro realizarán las tareas de registro presenciál, validación y procesado de las peticiones de certificados y de revocación/suspensión y renovación de certificados.

El proceso de petición y obtención de la tarjeta con los certificados de usuario es online y permite la expedición de la tarjeta de un usuario en tiempo real.

1.3.3 Suscriptores

Se entienden por usuarios de los certificados las entidades finales que hagan uso de los servicios de emisión y gestión de los certificados así como de los certificados mismos.

Los suscritores se diferencian en varios tipos:

- Solicitante: quien solicita el certificado, en su propio nombre o en nombre de una organización.
- Usuario: personas, dispositivos y organizaciones identificadas en el certificado.
- Poseedor de claves: personas físicas o dispositivos que posean de forma exclusiva las claves y estén autorizadas para su utilización. Las claves de cifrado pueden ser recuperadas por el prestador de servicios de certificación bajo determinadas condiciones.

En el ámbito del SESCAM los suscriptores de los certificados emitidos bajo está DPC podrán ser:

- Empleados de SESCAM o de sus entidades asociadas, bajo la clase 3 de certificados.
- Dispositivos electrónicos del SESCAM.

1.3.4 Terceros que confían en certificados

Aquellas personas físicas o jurídicas que reciben certificados emitidos por el SESCAM son terceros que confían en certificados y, como tales, les es de aplicación lo establecido por la presente Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados.

Se considera que los terceros confían en los certificados en función del empleo objetivo que de los mismos realicen en sus relaciones con los suscriptores. En este sentido deberá realizar las comprobaciones oportunas para que éste pueda establecer la relación de confianza en:

- Las firmas digitales realizadas por el suscriptor del certificado,
- En los procesos de control de acceso que requieran la autenticación del suscriptor mediante el certificado correspondiente asignado al mismo por el SESCAM.
- En el envío de elementos cifrados que requieren el uso del certificado del suscriptor por parte del tercero que confía en el mismo.

1.3.5 Otras entidades

El SESCAM admite el uso de certificados emitidos por otras Administraciones públicas españolas y europeas en los siguientes supuestos:

- Como elementos probatorios de identidad de los suscriptores en los procesos de registro remotos frenta a la infraestructura de clave pública.
- Reconocimiento de las firmas electrónicas de los suscritores de las mismas, siempre y cuándo éstas hayan sido realizadas con certificados cualificados y las firmas tengan la calificación de "reconocidas" según la especificación ETSI 101 456.

Para el reconocimiento de cualquier otra función o servicio se atenderá a los acuerdos firmados entre el SESCAM o los órganos competentes de la Junta de Comunidades de Castilla la Mancha.

1.4 Usos de los Certificados

Esta sección describe el tipo de aplicaciones para los que los certificados han sido emitidos, también explicita los tipos de aplicación inapropiada de éstos.

1.4.1 Usos apropiados de los certificados

El uso de cada uno de los certificados se encuentra explicado en el documento *"D.3.2.2 SESCAM – Políticas de Certificación"* bajo el epígrafe *"Comunidad de Aplicación".*

1.4.2 Usos prohibidos de los certificados

Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras

finalidades de las descritas para cada uno de ellos en *1.4.1 Usos apropiados de los certificados.*

1.5 Administración de la Declaración de Prácticas

1.5.1 Organización que administra el documento

Dirección de contacto:

C/ Huérfanos Cristinos, nº 5

45071 Toledo

Toledo

Tlfn: 925 27 41 00

Fax: 925 27 41 01

Email: info_pki@sescam.jccm.es

1.5.2 Detalles de contacto

Dirección de contacto:

C/ Huérfanos Cristinos, nº 5

45071 Toledo

Toledo

Tlfn: 925 27 41 00

Fax: 925 27 41 01

Email: info_pki@sescam.jccm.es

1.5.3 Persona que determina la conformidad de una Declaración de Prácticas de Certificación (DPC) con la política

Dirección de contacto:

C/ Huérfanos Cristinos, nº 5

45071 Toledo

Toledo

Tlfn: 925 27 41 00

Fax: 925 27 41 01

Email: info_pki@sescam.jccm.es

1.5.4 Procedimiento de aprobación de la DPC

El procedimiento de aprobación de la DPC se garantiza mediante la adecuada aplicación de los procedimientos correspondientes mantenidos por el SESCAM. Las modificaciones a la DPC son aprobadas por éste, después de verificar el cumplimiento definido en la sección *9.12 Correcciones a la DPC*.

2 Publicación de información y depósito de certificados

2.1 Deposito

Se entiende por depósito el sistema, o los sistemas, donde se publica la información relevante del SESCAM relativa a los servicios de la infraestructura de clave pública. El SESCAM dispone de diferentes depósitos o repositorios dependiendo del acceso que se requiera a los mismos, así pues los repositorios donde se encuentra la información disponible son:

1. Toda la información relativa a cada uno de los componentes que conforman la gestión de la emisión, revocación y suspensión de certificados está custodiada de forma segura e integra en las Bases de Datos de las Autoridades de Certificación.

2. Repositorio WEB, donde se podrá encontrar la documentación que rige la operativa de la infraestructura y las listas de revocación de la Autoridad de Certificación del SESCAM.

3. Directorios LDAP donde la Autoridad de certificación pública los certificados que deben ser publicados atendiendo a la política de certificación a la que están asociados.

El acceso a estos sistemas se encuentra disponible los 7 días x 24 horas del año, salvo acciones de mantenimiento preventivo o correctivo que pudieran acontecer.

2.1.1 Publicación de información de la Autoridad de Certificación

La Autoridad de Certificación publicará la siguiente información:

- La declaración de practicas de certificación (DPC) en http://sescam.jccm.es/pki/dpc/dpc.pdf.
- Las políticas de certificación (PC) en http://sescam.jccm.es/pki/dpc/pc.pdf
- El certificado de las Autoridades de Certificación:
    - Todos los Dominios de Windows pertenecientes al SESCAM y a sus entidades asociadas bajo las ramas:
        - CA raíz

- ldap:///CN=SESCAM-ROOT-CA, CN=Certification Authorities, CN=Public Key Services, CN=Services, CN=Configuration, DC=*<Controlador de Dominio >*, DC=com?cACertificate?base?objectclass=certificationAuthority
- ldap:///CN=SESCAM-ROOT-CA, CN=AIA, CN=Public Key Services, CN=Services, CN=Configuration, DC=*<Controlador de Dominio >,* DC=com?cACertificate?base?objectclass=certificationAuthority

- Autoridad de Certificación Subordinada
  - ldap:///CN=SESCAM-SUB-CA, CN=AIA, CN=Public Key Services, CN=Services, CN=Configuration, DC=*<Controlador de Dominio >,* DC=com?cACertificate?base?objectclass=certificationAuthority

- Directorio Público del SESCAM bajo la clase auxiliar `certificationAuthority, en:`
  - `CA Raíz`
    - *ldap://*servldap.sescam.jclm.es*/o=SESCAM Root CA,dc=sescam,dc=jclm,dc=es*?cACertificate?base?objectclass=certificationAuthority
  - `CA Subordinada`
    - *ldap://*servldap.sescam.jclm.es*/o=SESCAM Subord CA,dc=sescam,dc=jclm,dc=es*?cACertificate?base?objectclass=certificationAuthority
- `Repositorio WEB del SESCAM en:`
  - CA Raíz
    - http://sescam.jccm.es/pki/certs/sescam_root_ca.crt
  - CA Subordinada
    - http://sescam.jccm.es/pki/certs/sescam_subord_ca.crt

- Las listas de revocación de los certificados (LCR) en:
  - El directorio público del SESCAM bajo la clase auxiliar `certificationAuthority`, en el atributo `certificateRevocationList`
    - CA Raíz
      - *ldap://*servldap.sescam.jclm.es*/o=SESCAM Root CA, dc=sescam, dc=jclm, dc=es* ?authorityRevocationList?base?objectclass=certificationAuthority
    - *CA Subordinada*

- *ldap://*servldap.sescam.jclm.es*/o=SESCAM Subord CA,dc=sescam,dc=jclm,dc=es*?certificateRevocationList?base?objectclass=certificationAuthority

- En el repositorio web del SESCAM
  - CA Raíz
    - http://sescam.jccm.es/pki/crls/sescam_root_ca.crl
  - CA Subordinada
    - http://sescam.jccm.es/pki/crls/sescam_subord_ca.crl
  - Certificados de Entidad Final, solamente serán publicados los certificados pertenecientes a la política de la clase 3, Política de EF de Empleados de Cifrado, en el directorio público del SESCAM, bajo el atributo userCertificate del usuario al que pertenece y cuya entrada existe y es mantenida por el SESCAM.

2.1.2 Frecuencia de Publicación

La Declaración de Prácticas de Certificación (DPC) y las políticas de certificación (PC) se publicarán en cuanto se encuentran disponibles y los correspondientes cambios se gestionarán según lo establecido en este documento en la sección 9.1.12.

Las listas de revocación (LCR) se publicarán siguiendo los procedimientos definidos en la sección 4.9.7 de este documento.

Los certificados de entidad final susceptibles de ser publicados, lo serán por la Autoridad de Certificación en el momento de su emisión.

2.1.3 Control de acceso

No se necesitan controles de acceso de lectura sobre la declaración de prácticas de certificación (DPC) y las políticas de certificación (PC) en la ubicación utilizada por la publicación.

Los certificados de las Autoridades de Certificación y sus LCR están también disponibles únicamente para consultas.

Los certificados de los usuarios del SESCAM publicados están disponibles con acceso de lectura para el entorno cerrado del SESCAM.

Únicamente el personal autorizado puede añadir, modificar o borrar datos.

El acceso a las Bases de Datos gestionadas por la Autoridad de Certificación estará únicamente disponible para el personal autorizado a tal fin.

3 IDENTIFICACION Y AUTENTICACION

3.1 Registro inicial

3.1.1 Tipos de nombres

Todos los certificados requieren un nombre distinguido en el campo Subject Name que cumpla con lo definido en el estándar x.501 para "Distinguished Names".

En el caso de certificados de Entidad Final el operador de registro verificará los nombres distinguidos de la solicitud en el momento de generar la petición de certificación.

3.1.2 Significado de los nombres

En los certificados de empleado el nombre del suscriptor estará compuesto al menos por su nombre y apellidos, pudiendo incluir el cargo que ocupa dentro de la organización, así como también el identificador único dentro del directorio LDAP del SESCAM.

En los certificados de dispositivo de servidor el nombre del suscriptor es el nombre del dominio, la dirección IP del servidor o el nombre que esté indicado en la petición.

En el certificado de firma de código, en el nombre del suscriptor se indica el nombre del órgano competente o de la entidad a la que pertenece el software.

3.1.3 Utilización de anónimos y pseudónimos

No se permite la utilización de anónimos ni seudónimos en ningún caso.

3.1.4 Interpretación de formatos de nombres

No se establecen estipulaciones adicionales para la interpretación de nombres.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores son únicos para cada tipo de certificado (Política de certificación) emitido.

3.1.6 Reconocimiento, Autenticación y resolución de conflictos relativos a nombres

Los solicitantes de certificados no pueden incluir nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

El SESCAM determinará para los certificados de dispositivo físico y firma de código que el solicitante de certificado tiene derecho sobre el nombre que aparece en una solicitud del mismo, siempre y cuando éste pertenezca al entorno operativo del SESCAM, la emisión de certificados de estas clases fuera del ámbito del SESCAM queda estrictamente prohibida por lo que no es de aplicación la verificación del nombre.

3.2 Validación inicial de la Indentidad

3.2.1 Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de generación de claves, petición de certificado y entrega del mismo al soporte criptográfico donde las claves están almacenadas.

El documento de políticas de certificación *"D3.2.2 SESCAM – Politicas de Certificación"* describe el procedimiento de prueba de posesión de clave privada exigido para cada Clase y Tipo de certificado recogido en la presente DPC.

3.2.2 Autenticación de la identidad de una Organización

No se requiere realizar procedimiento de autenticación de la organización titular del certificado en certificados de Clase 4, ya que se trata de certificados corporativos, en los que la organización o entidad suscriptora del certificado pertenece a la organización. Sin embargo, si será necesario comprobar que el dispositivo electrónico que se desea certificar existe y que el solicitante de la misma dispone de la autorización necesaria para exigirlo.

En el caso de certificados de Clase 5, certificados de firma de código, será de aplicación el mismo procedimiento.

3.2.3 Autenticación de la identidad de una persona física

La identificación y acreditación de las personas físicas exige la personación de las mismas ante los Operadores de Registro y la presentación de la siguiente documentación:

- Acreditación corporativa del SESCAM
- Documento Nacional de Identidad

No se contemplan procedimientos de acreditación que no requieran la presencia personal al realizarse el proceso de registro y certificación en tiempo real concluyéndose con la entrega de la tarjeta con claves y certificados operativos al usuario.

3.2.4 Información de suscriptor no verificada

El SESCAM no se responsabiliza de la veracidad de toda la información incluida en la solicitud de certificado, así como tampoco de que la misma sea completa, o que tenga derecho a su uso.

3.2.5 Validación de Autoridad

El operador de registro del SESCAM velará porque las autorizaciones presentadas por solicitantes en nombre de elementos de la organización sean válidas y fehacientes, estableciendo los mecanismos oportunos para que así sea.

3.2.6 Criterios de Interoperabilidad

No se definen criterios de interoperabilidad entre la AC del SESCAM y otras. Los mecanismos deberán ser establecidos de forma bilateral e independiente con otras Autoridades de Certificación.

3.3 Identificación y autenticación para peticiones de renovación de claves

3.3.1 Registro para renovación rutinaria de claves y certificados

Para renovar un certificado se tendrá que solicitar uno nuevo siguiendo el proceso de solicitud y emisión de certificado establecido para cada clase y tipo de certificado tal y como se describe en el documento *"D3.2.2 SESCAM – Politicas de Certificación"*, sección "Requerimientos Operacionales".

3.3.2 Registro para renovación de claves y certificados tras revocación

Tras la revocación de un certificado se tendrá que solicitar uno nuevo siguiendo el proceso de solicitud y emisión de certificado establecido para cada clase y tipo de certificado tal y como se describe en el documento *"D3.2.2 SESCAM – Politicas de Certificación"*, sección "Requerimientos Operacionales".

3.4 Identificación y autenticación para peticiones de revocación.

Las peticiones de revocación de un certificado vendrán determinadas por los establecido para cada clase y tipo de certificado tal y como se describe en el documento *"D3.2.2 SESCAM – Politicas de Certificación"*, sección "Requerimientos Operacionales".

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 Solicitud de certificados

4.1.1 Quién puede solicitar certificados

La solicitud es el primer paso que debe llevar a cabo un suscriptor del SESCAM para conseguir certificados.

Esta solicitud requiere el envío de un documento con la información exacta y comprobada (certificada) de las personas o dispositivos para las que se pide el certificado. Esta solicitud se firma por la persona autorizada por el suscriptor, en caso de tratarse de un dispositivo.

Sólo aquellas personas, instituciones, entidades o dispositivos del SESCAM podrán solicitar certificados de éste.

4.1.2 Procedimiento de alta y Responsabilidades

El SESCAM o el centro asociado que recibe la solicitud de certificación es responsable de realizar el procedimiento de alta de la misma. Esta información será dada de alta en la base de datos de la autoridad de registro con el fin de realizar consultas posteriores, sobre el estado de la solicitud o de los certificados de un suscriptor particular.

4.2 Procesamiento de la solicitud de certificación

En el momento en que el SESCAM o una de sus entidades asociadas recibe una solicitud de certificado de clase 3 se procede al registro de la misma, bien mediante la aplicación de registro correspondiente asociada a la Autoridad de Certificación, bien mediante el uso de la aplicación corporativa, GESUSER.

Durante el proceso de solicitud existe una comprobación de que el usuario o dispositivo realmente pertenece al sistema, dicha comprobación es llevada a cabo mediante consulta al directorio corporativo del SESCAM, donde necesariamente debe encontrarse la información del suscriptor solicitante.

4.2.1 Procesamiento de solicitud de certificados de Autoridad de Certificación

Para la solicitud de creación de autoridades de certificación de nivel 2 o producción asociada a certificados de clase 2, será necesario que las mismas generen un conjunto de claves en dispositivo hardware criptográfico homologado cómo mínimo a FIPS 140-1 nivel 2, los Oficiales de Seguridad de estás entidades entregarán la solicitud de certificado en formato PKCS# 10 o X509 autofirmado a los Oficiales Regístrales de la Autoridad de Certificación Raíz, quienes deberán velar por la correcta identificación del suscriptor y sus representantes, y de la autenticidad de la información que se le presenta en la solicitud.

El tiempo de procesamiento de estas solicitudes estará en función de la disponibilidad del conjunto de Oficiales de Registro necesario para procesar dicha solicitud.

4.2.2 Procesamiento de solicitud de certificados de personas físicas

El solicitante deberá personarse en la Entidad de Registro para solicitar sus certificados acreditándo su identidad corporativa del SESCAM y DNI. La solicitud de la tarjeta de un empleado del SESCAM se podrá realizar remotamente a través de la aplicación GESUSER (procedimiento normal de uso) o mediante la propia Autoridad de Registro del centro (SESCAM, hospital , etc).

Los certificados de persona física corresponden a aquellos englobados dentro de la clase 3 que está Declaración recoge. La emisión de certificado de esta clase esta asociada a la entrega de un dispositivo criptográfico al usuario, y requiere la emisión de los tres tipos de certificados, es decir, en el proceso de solicitud el suscriptor obtendrá los tres certificados en su tarjeta electrónica para los procesos de autenticación, no-repudio y confidencialidad.

El tiempo de procesamiento de estas peticiones tendrá carácter inmediato, al personarse el suscriptor en los puntos de registro presénciales habilitados a tal efecto.

4.2.3 Procesamiento de solicitud de certificados de dispositivo

Para la solicitud de certificados de clase 4, servidor WEB y de Controlador de dominio Windows, así como también de los certificados de clase 5, de firma de código, las claves se generan por los mecanismos propios de estos dispositivos y sus administradores entregan en la Entidad de Registro la petición de certificación en formato PKCS# 10 junto a la clave pública para su certificación según el procedimiento descrito en 4.3 Emisión de certificados.

El tiempo de procesamiento de estás solicitudes será cómo máximo de 2 días laborales.

4.3 Emisión de certificados

4.3.1 Procedimiento de la Infraestructura para la emisión de certificados

Este apartado describe las acciones llevadas a cabo por los elementos regístrales, es decir, Operador de Registro y/o Aplicación de Registro GESUSER, Autoridad de Registro y la Autoridad de Certificación. Se indica el procedimiento aplicado por cada uno de los elementos para validarse entre si, validar la solicitud de certificación y emitir los correspondientes certificados.

4.3.1.1 Emisión de Certificados de Autoridad de Certificación Subordinada

Una vez recibida una solicitud de estás características, un conjunto determinado de Oficiales de Registro procederá a la generación de certificado mediante la presentación de sus respectivas credenciales a la Autoridad de Certificación Raíz.

La emisión de certificados de esta clase sólo se podrá realizar localmente en la CA Raíz del SESCAM, mediante el siguiente procedimiento:

1 Un conjunto de operadores de registro con los permisos adecuados iniciará sesión en la aplicación de administración de la CA Subordinada del SESCAM.

2 Estos operadores de la CA procesará la petición generada por los oficiales de Seguridad de la CA subordinada aplicando el correspondiente perfil de certificación, exportará en un fichero el certificado emitido y se lo entregará a os oficiales de seguridad de la CA Subordinada.

3 Los oficiales de Seguridad instalarán el certificado contenido en el fichero entregado en éstos usando las aplicaciones de administración correspondientes de la CA subordinada.

4.3.1.2 Emisión de Certificados de Persona Física

4.3.1.2.1 Procedimiento de emisión certificados clase 3 de un usuario a través de la aplicación GESUSER.

1 El operador de la aplicación GESUSER se conectará a ésta mediante su navegador Web y se autenticará según los mecanismos establecidos para el uso de la misma.

2 El operador de la aplicación GESUSER ordenará a ésta la generación de la tarjeta de un determinado usuario del centro.

3 La aplicación GESUSER establecerá una conexión HTTPS con un determinado servicio de la AR del centro, autenticándose con un certificado configurado en la AR.

4 La aplicación GESUSER enviará una petición XML de solicitud de tarjeta de un usuario a la AR del centro, conteniendo la dirección de
correo electrónico y la fotografía del usuario, el PIN y el PUK de la tarjeta y el identificador del conjunto de impresoras a utilizar en la emisión de la tarjeta.

5 El servicio de la AR procesará la petición XML recibida mediante el siguiente procedimiento:

a) Buscará en una determinada rama del LDAP SESCAM los valores de los atributos `title`, `uid` y `cn` de una entrada de clase `inetOrgPerson` y con un valor del atributo `mail` igual a la dirección de correo electrónico contenida en la petición XML. Si no encuentra la entrada o ésta no contiene los atributos `title`, `uid` y `cn`, devolverá una respuesta conteniendo el correspondiente error.

b) Buscará en una determinada rama del Active Directory del centro el valor del atributo `userPrincipalName` (*UPN*) del usuario con un valor del atributo `mail` igual a la dirección de correo electrónico contenida en la petición XML. Si no encuentra la entrada en el Active Directory, indicado igualmente en la petición XML, o ésta no contiene el atributo `userPrincipalName`, devolverá una respuesta conteniendo el correspondiente error.

c) Buscará en la tabla de peticiones de tarjetas de la AR del centro un registro conteniendo una dirección de correo electrónico igual a la contenida en la petición XML. Si encuentra el registro, dependiendo del estado contenido en el mismo realizará lo siguiente:

- Estados *Pending* o *En proceso*: devolverá una respuesta conteniendo el correspondiente error (se ha recibido con anterioridad una solicitud de tarjeta para el usuario y aún no se ha finalizado su generación).
- Estado *Finalizada con errores*: borrará el registro (se creará uno nuevo).
- Estados *Finalizada con éxito* o *Suspendida*: si los certificados del usuario están expirados (el registro contiene la fecha y hora de expiración de los mismos), borrará el registro (se creará uno nuevo); en otro caso, devolverá una respuesta conteniendo el correspondiente error (el usuario ya tiene una tarjeta válida o suspendida)

d) Creará un registro en una tabla de peticiones de tarjetas de la AR del centro, conteniendo los datos recibidos en la petición XML (dirección de correo electrónico, fotografía, identificador del conjunto de impresoras, PIN y PUK1), los datos buscados en el LDAP SESCAM (Title, UID y CN) y en el Active Directory del centro (UPN) y el estado Pendiente. Si el nuevo registro se ha almacenado correctamente en la tabla de peticiones de tarjetas de la AR del centro, devolverá una respuesta indicando que la solicitud de tarjeta del usuario ha sido aceptada. En otro caso, devolverá una respuesta conteniendo el correspondiente error.

6 Posteriormente, la tarjeta será emitida por una tarea desatendida de la AR del centro (tarea de emisión de tarjetas). Esta tarea consultará periódicamente la tabla de peticiones de tarjetas y emitirá las tarjetas de los usuarios correspondientes a los registros con estado *Pendiente*, mediante el siguiente proceso:

a. Modificará el registro, cambiando su estado a *En Proceso*.

b. Cargará una tarjeta en la impresora de tarjetas del conjunto de impresoras con el identificador contenido en el registro.

c. Generará 2 pares de claves (pública y privada) en la tarjeta (claves de autenticación y de no repudio).

d. Creará las siguientes peticiones en la tabla de peticiones de la AR, usando los datos contenidos en el registro (dirección de correo electrónico, *Title*, *CN*, *UID*, *UPN*)

- Una petición del certificado de autenticación del usuario conteniendo una de las claves públicas generadas en la tarjeta, según el perfil especificado en el documento de políticas *"D3.2.2 SESCAM – Políticas de Certificación"*, capítulo 4, sección *"Perfil de Certificado EF Empleado Autenticación"*

- Una petición del certificado de no repudio del usuario conteniendo la otra clave pública generada en la tarjeta, según el perfil especificado en el documento de políticas *"D3.2.2 SESCAM – Políticas de Certificación"*, capítulo 4, sección *"Perfil de Certificado EF Empleado No- Repudio"*

- Una petición de PKCS#12 (sin cadena de certificación ni certificado raíz) para el certificado de cifrado del usuario, según el perfil especificado en el documento de políticas *"D3.2.2 SESCAM – Políticas de Certificación"*, capítulo 4, sección *"Perfil de Certificado EF Empleado Cifrado"*

e. Modificará el registro, añadiendo los identificadores de las 3 peticiones creadas en la tabla de peticiones de la AR.

---

[1] *El PIN y el PUK se almacenarán cifrados (ofuscados) en el registro y son borrados de forma segura y fehaciente de éste un vez que se usen para cambiar los que vienen por defecto en la tarjeta*

f. Generará un lote con las 3 peticiones creadas en la tabla de peticiones de la AR y lo enviará al servicio de procesado de lotes de la CA Subordinada. El lote de respuesta generado por la CA Subordinada contendrá los 3 certificados solicitados (no contendrá el PKCS#12 correspondiente al certificado de cifrado del usuario). Las claves correspondientes al certificado de cifrado del usuario habrán sido generadas y archivadas cifradas (ofuscadas) por la CA Subordinada. El certificado de cifrado habrá sido publicado en la entrada del usuario en el LDAP SESCAM por la CA Subordinada.

   Si se produce un error durante los pasos b y e (por ejemplo, no hay tarjetas en el cargador, la tarjeta cargada está defectuosa o al revés o el servicio de procesado de lotes de la CA Subordinada no está accesible), realizará las siguientes acciones:

   - Expulsará la tarjeta de la impresora (si la ha cargado).
   - *Mo*dificará el registro, cambiando su estado a *Finalizado con errores* y añadiendo la causa del error.
   - Finalizará el proceso de emisión de la tarjeta.

g. Recuperará un PKCS#12 del certificado de cifrado del usuario (identificado por el número de serie del certificado) y la contraseña aleatoria que lo protege, mediante una petición a un servicio de entrega de claves de la CA Subordinada.

h. Insertará en la tarjeta los certificados de autenticación y de no repudio del usuario y el PKCS#12 del certificado de cifrado del usuario.

i. Cambiará el PIN y el PUK de la tarjeta (PIN y PUK por defecto) por los que están almacenados cifrados (ofuscados) en el registro.

j. Modificará el registro, borrando el PIN y el PUK almacenados en el mismo.

k. Imprimirá físicamente la tarjeta por sus dos caras de acuerdo al diseño gráfico especificado en el apéndice A (la tarjeta inicialmente estará completamente en blanco), donde NOMBRE Y APELLIDOS, CARGO y FOTOGRAFÍA serán respectivamente los datos CN, Title y fotografía contenidos en el registro.

   Si se produce un error durante los pasos f y j (por ejemplo, el servicio de entrega de claves de la CA Subordinada no está accesible, el PIN y el PUK de la tarjeta no son el PIN y el PUK por defecto o se ha acabado el cartucho de tinta de la impresora), realizará las siguientes acciones:

   - Generará un lote conteniendo la revocación de los 3 certificados emitidos del usuario (localizados en la tabla de peticiones de la AR a partir de los identificadores contenidos

en el registro de la tabla de peticiones de tarjetas) y lo enviará al servicio de procesado de lotes de la CA Subordinada (se revocarán inmediatamente los 3 certificados del usuario).

- Expulsará la tarjeta de la impresora.
- Modificará el registro, cambiando su estado a Finalizado con errores y añadiendo la causa del error.
- Finalizará el proceso de emisión de la tarjeta.

l. Expulsará la tarjeta de la impresora y modificará el registro cambiando su estado a Finalizado con éxito y añadiendo la fecha y hora de expiración de los 3 certificados del usuario (es la misma para los 3 certificados)

- Siempre que la impresora expulse una tarjeta impresa físicamente por sus 2 lados, se podrá tener la seguridad de que se ha generado correctamente.
- Siempre que la impresora expulse una tarjeta no impresa físicamente por sus 2 lados, se podrá tener la seguridad de que no se ha generado correctamente y de que si se han emitido los certificados del usuario éstos estarán revocados. El contenido de la tarjeta dependerá del momento en que se ha producido el error, pudiendo estar vacía, contener sólo claves o contener claves y certificados (si se quiere reutilizar la tarjeta, antes se deberá borrar manualmente su contenido, si lo hubiere).

m. Imprimirá un papel en la impresora láser conteniendo un contrato de uso de la tarjeta generada. El contrato contendrá, al menos, el nombre y apellidos del usuario (dato *CN* contenido en el registro de la tabla de peticiones de tarjetas).

- Si se produce un error en la impresión del contrato, no se realizará ninguna acción (en este caso, el contrato deberá ser impreso manualmente por el operador de la aplicación GESUSER).

7 El operador de la aplicación GESUSER podrá consultar en todo momento el estado de la solicitud de la tarjeta del usuario mediante el siguiente procedimiento:

a. El operador de la aplicación GESUSER ordenará a ésta la consulta del estado de la solicitud de la tarjeta de un determinado usuario del centro.

b. La aplicación GESUSER enviará una petición XML de estado de solicitud de la tarjeta de un usuario a la AR del centro, conteniendo la dirección de correo electrónico del usuario.

c. El servicio de la AR buscará en la tabla de peticiones de tarjetas de la AR del centro un registro conteniendo una dirección de correo electrónico igual a la contenida en la petición XML. Si no encuentra el registro, devolverá una

respuesta conteniendo el correspondiente error. En otro caso, devolverá una respuesta conteniendo el estado almacenado en el registro (*Pendiente*, *En proceso*, *Finalizada con éxito*, *Finalizada con errores* o *Suspendida*).

4.3.1.2.2 Procedimiento de emisión de la tarjeta de un usuario en la AR del centro

1 Un operador con los permisos adecuados iniciará sesión en la aplicación de administración de la AR del centro.

2 El operador de la AR ordenará a ésta la generación de la tarjeta de un determinado usuario del centro, indicando la dirección de correo electrónico y la fotografía del usuario, el PIN y el PUK de la tarjeta y el identificador del conjunto de impresoras a utilizar en la emisión de la tarjeta.

3 La AR registrará la petición en la tabla de peticiones de tarjeta de la AR del centro, usando el mismo procedimiento que realiza el servicio de la AR (paso 5 del procedimiento de emisión de la tarjeta de un usuario a través de la aplicación GESUSER, página 22), mostrando por pantalla el resultado de la operación (contenido de la respuesta XML del servicio).

4 Posteriormente, la tarjeta será emitida por la tarea de emisión de tarjetas (paso 5 del procedimiento de emisión de la tarjeta de un usuario desde la aplicación GESUSER, página 22).

5 El operador de la AR del centro podrá consultar en todo momento el estado de la solicitud de la tarjeta del usuario (podrá consultar los datos de los registros de la tabla de peticiones de tarjeta de la AR).

4.3.1.3 Emisión de Certificados de Dispositivo

La emisión de certificados de clase 4, servidor WEB y Controlador de dominio Windows, asi como de clase 5, firma de código, sólo se podrá realizar localmente en la CA Subordinada del SESCAM, mediante el siguiente procedimiento:

1 Un operador con los permisos adecuados iniciará sesión en la aplicación de administración de la CA Subordinada del SESCAM.

2 El operador de la CA procesará la petición generada por el administrador del dominio aplicando el correspondiente perfil de certificación, exportará en un fichero el certificado emitido y se lo entregará al administrador del dominio.

3 El administrador del servidor web, del dominio o del software objeto de certificación instalará el certificado contenido en el fichero entregado en éste usando las aplicaciones de administración correspondientes.

4.3.2 Notificación a suscriptores de la emisión de certificados

La Autoridad de Certificación del SESCAM sólo notificará la emisión de certificados o incidencias en el proceso para los certificados de clase 4 y 5. El resto de certificados requiere la presencia física del suscriptor por lo que no se requiere un proceso de notificación por parte de la Autoridad de Certificación.

4.4 Aceptación de certificados

4.4.1 Conducta que constituye aceptación de certificado

La entrega del contrato de aceptación, la tarjeta criptográfica y la activación de la misma con el PIN y el PUK elegidos por el suscriptor o poseedor de las claves se considera como aceptación de los certificados de EF para persona física y de la las obligaciones definidas en esta DPC.

Para los certificados de dispositivo y firma de código, se establece el uso inicial del mismo como elemento de aceptación.

4.4.2 Publicación del certificado

Los certificados se pueden publicar sin el consentimiento previo de los poseedores de claves. En el caso particular de certificados de personas físicas siempre serán publicados los certificados correspondientes a la Política de EF de Empleado para Cifrado.

4.4.3 Notificación de la emisión a terceros

No es de aplicación.

4.5 Uso del par de claves y del certificado

En el entorno operativo del SESCAM, se ha requerido la implantación de mecanismos de seguridad que permitan una adecuada gestión de la información:

1 Privacidad de la información, en este sentido existen diversos aspectos que deben considerarse, entre los que cabe destacar por ejemplo: cumplimiento con requisitos de la LOPD en el uso de comunicaciones cifradas, garantía de privacidad a expedientes médicos, etc.

2 Control de acceso, a instalaciones, servicios informáticos y/o recursos informáticos específicos que requieran privilegios y posterior auditoría.

3 No repudio, basada actualmente en la firma por parte de diferentes perfiles como mecanismo revisor, autorizador, etc. Este mecanismo ampliamente utilizado y reconocido, por ejemplo cuando el médico firma una receta, un expediente, una solicitud de servicio asistencial, etc, puede ser sustituida por una firma digital con reconocimiento, agilizando los procesos y produciendo un ahorro en recursos materiales.

4 Securización de las comunicaciones mediante correo electrónico entre los distintos centros del SESCAM, así como con otros Departamentos, de acuerdo a las relaciones de confianza que se puedan establecer.

5 Dotar de mayores medidas de seguridad el acceso a la red de área local de los servicios Centrales del SESCAM, así como de los hospitales.

En este sentido los certificados y sus claves asociadas se utilizan para garantizar la calidad y seguridad de estos requerimientos.

4.5.1 Uso por los poseedores de claves

Los certificados se utilizan de acuerdo con su función propia y finalidad establecida, y no se pueden utilizar en otras funciones o con otras finalidades.

Dichos usos quedan descritos en el documento "*D3.2.2 SESCAM – Políticas de Certificación",* capítulo 2, *"Comunidad de aplicación",* para cada una de las clases y tipos de certificados recogidos en esta DPC.

4.5.2 Uso por el tercero que confía en certificados

El uso por parte de terceros de los certificados emitidos por el SESCAM deberán estar de acuerdo con el carácter y la funcionalidad para la que fueron emitidos, el uso de los mismos para fines distintos de los recogidos en el documento "*D3.2.2 SESCAM – Políticas de Certificación",* capítulo 2, *"Comunidad de aplicación",* para cada una de las clases y tipos de certificados recogidos en esta DPC queda estrictamente prohibida.

4.6 Renovación de certificados sin renovación de claves

No se permite proceso de renovación para el conjunto de certificados del SESCAM.

4.7 Renovación de certificados con renovación de claves

4.7.1 Renovación de Certificados de Personas físicas

El proceso de renovación está ligado al de la tarjeta del usuario de un hospital o del SESCAM se considera igual a una emisión de una nueva tarjeta del suscriptor una vez que su anterior tarjeta ha expirado, tal y como queda reflejado en "4.3.1.2 Emisión de Certificados de Persona Física" de esta DPC.

Sólo se permitirá emitir una nueva tarjeta de suscriptor del SESCAM antes de que su anterior tarjeta haya expirado si ésta ha sido revocada.

4.7.2 Renovación de Certificados de Dispositivo o de Firma de Código

Sólo se permitirá emitir un nuevo certificado de esta clase antes de que su anterior certificado haya expirado si éste ha sido revocado, en cualquier caso constituirá una nueva emisión de certificado que requerirá también que se hayan generado nuevas claves.

4.8 Modificación de Certificado

Esta DPC requiere la revocación y nueva emisión de certificados si estos requieren cualquier tipo de modificación.

4.9 Revocación y Suspensión de certificados

4.9.1 Supuestos de revocación

Los certificados emitidos por el SESCAM se revocarán en los siguientes casos:

- Solicitud voluntaria del suscriptor o posesor de claves.
- Solicitud de la Autoridad de Certificación.
- Inexactitudes en el certificado.
- Pérdida o inutilización por daños del soporte del certificado.
- Compromiso o sospecha de compromiso de seguridad de las claves o del soporte en el que las mismas se encuentran.

- Utilización indebida del certificado.
- Fallecimiento o incapacidad sobrevenida, total o parcial, del posesor de claves del certificado.
- Perdida de condición de empleado del SESCAM.
- Extinción o cese de la actividad por parte de la Autoridad de Certificación o revocación de sus claves.

4.9.2 Entidades que pueden solicitar la revocación

Las peticiones de revocación pueden ser realizadas por:

- El operador de Entidad de Registro previa petición del suscriptor o poseedor de claves.
- El Administrador de la Autoridad de Certificación previa petición y autorización de los oficiales de seguridad del SESCAM.

4.9.3 Procedimiento de revocación

En el caso de que la petición de revocación sea presentada por el suscriptor o poseedor de claves el operador de la Entidad de Registro tendrá que identificarlo siguiendo los procedimientos definidos en la sección 3.2.

Si la identificación da resultado positivo el operador de la Entidad de Registro pedirá la razón de la revocación y activará el proceso de revocación:

- Selección del certificado o certificados afectados.
- Generación del lote con la petición de revocación (o las peticiones) y envió a la Autoridad de Certificación.
- Procesado del lote por la Autoridad de Certificación y generación de la nueva Lista de revocación.

Con este procedimiento la revocación de los certificados se realiza con un proceso en línea y la generación y publicación de la Lista de Revocación es inmediata.

En el caso de que la petición de revocación sea presentada por los responsables seguridad del SESCAM un Oficial de Registro de la Autoridad de Certificación procederá a la revocación del certificado (o certificados) afectado y a la generación de la nueva lista de revocación.

Siempre que se proceda a la revocación de certificados de una persona física se tendrá que revocar el conjunto de todos sus certificados (ie, para un empleado del SESCAM: Autenticación, No-Repudio y Cifrado).

4.9.4 Periodo para la solicitud de revocación

El suscriptor del certificado deberá realizar la solicitud de revocación tan pronto le sea posible una vez se haya producido la causa de la misma.

4.9.5 Periodo de procesamiento de la solicitud de revocación por parte de la CA

La solicitud de revocación una vez llega a uno de los operadores de registro del SESCAM se procesa en el tiempo mínimo posible, con carácter de inmediatez, y siempre dentro de los horarios laborales de los departamentos de registro del SESCAM.

4.9.6 Obligación de consulta de información de revocación de certificados

Los terceros que aceptan certificados del SESCAM podrán verificar el estado de los mismos accediendo al punto de distribución de las listas de revocación del SESCAM, dicha información de localización se encuentra en el propio certificado que se pretende verificar.

SESCAM no impone la obligatoriedad de comprobar el estado de los certificados si bien recomienda la verificación de los mismos.

4.9.7 Frecuencia de emisión de listas de certificados revocados

Las listas de revocación se emiten cada vez que un certificado es revocado o suspendido y se publican como está indicado en *"2.1.2 Frecuencia de Publicación"*.

El SESCAM emite una lista de revocación al menos cada día.

4.9.8 Tiempo de latencia máximo entre LCRs

Una vez se haya producido una revocación, la autoridad de certificación generará una nueva lista de certificados revocados, que sustituirá a la vigente. La nueva lista de certificados revocados será publicada en el lugar de la antigua tal como se establece en *"2.1.1 Publicación de información de la Autoridad de Certificación"* en un plazo no superior a **una hora**.

4.9.9 Disponibilidad Online de los servicios de comprobación de estado de certificados.

Las listas de revocación pueden ser consultadas en al menos dos repositorios diferentes tal y como se indica en "2.1.1 Publicación de información de la Autoridad de Certificación".

La disponibilidad de ambos repositorios está diseñada para dar servicio 24x7x365.

Actualmente SESCAM no provee servicios de validación en línea propiamente dichos, como OCSP (Online Certificate Status Protocol) definidos por la RFC 2560.

4.9.10 Requerimientos de comprobación online del estado de los certificados

No aplicable.

4.9.11 Otros mecanismos de información de revocación de Certificados.

Sin estipular.

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

En caso de compromiso de la clave privada del certificado el suscriptor/poseedor de claves deberá notificar la circunstancia a la Autoridad de Registro para que se proceda a solicitar la revocación del certificado, o certificados en el caso de que éste pertenezca a persona física.

En caso de compromiso de la clave privada de la CA del SESCAM, se procederá de acuerdo a lo establecido en la sección 5.7.3. de esta DPC.

4.9.13 Supuestos de suspensión

Los certificados de persona física emitidos por el SESCAM se podrán suspender de forma cautelar cuando existan indicios sobre la existencia de una causa de revocación.

El resto de certificados contemplados en esta DPC no son susceptibles de suspensión temporal.

4.9.14 Entidades que pueden solicitar la suspensión

Las peticiones de suspensión pueden ser realizadas por:

- El operador de Entidad de Registro previa petición del suscriptor o poseedor de claves.
- El Administrador de la Autoridad de Certificación previa petición y autorización de los oficiales de seguridad del SESCAM.

4.9.15 Procedimiento de suspensión

La suspensión de un certificado de empleado, asociado a la tarjeta de un usuario de un hospital o del SESCAM, se podrá realizar remotamente a través de la aplicación GESUSER (procedimiento normal de uso) o localmente en la AR del centro (hospital o SESCAM).

4.9.15.1 Procedimiento de suspensión de la tarjeta de un usuario a través de la aplicación GESUSER

1 El operador de la aplicación GESUSER se conectará a ésta mediante su navegador Web y se autenticará según los mecanismos establecidos para el uso de la misma.

2 El operador de la aplicación GESUSER ordenará a ésta la suspensión de la tarjeta de un determinado usuario del centro.

3 La aplicación GESUSER establecerá una conexión HTTPS con un determinado servicio de la AR del centro, autenticándose con un certificado configurado en la AR.

4 La aplicación GESUSER enviará una petición XML de suspensión de la tarjeta de un usuario a la AR del centro, conteniendo la dirección de
correo electrónico del usuario.

5 El servicio de la AR procesará la petición XML recibida mediante el siguiente procedimiento:

a) Buscará en la tabla de peticiones de tarjetas de la AR del centro un registro conteniendo una dirección de correo electrónico igual a la contenida en la petición XML y el estado *Finalizada con éxito*

- Si no encuentra el registro, devolverá una respuesta conteniendo el correspondiente error (el usuario no tiene tarjeta o ésta ha sido revocada).
- Si encuentra el registro y el estado contenido en el mismo no es *Finalizada con éxito*, devolverá una respuesta conteniendo el correspondiente error:
- Estados *Pending* o *En proceso*: no se puede suspender la tarjeta porque aún no se ha finalizado su generación.

- Estado *Finalizada con errores*: no se puede suspender la tarjeta porque sus certificados no han sido emitidos o han sido revocados.

b) Estado *Suspendida*: no se puede suspender la tarjeta porque sus certificados ya han sido suspendidos.

c) Generará un lote conteniendo la suspensión de los 3 certificados emitidos del usuario (localizados en la tabla de peticiones de la AR a partir de los identificadores contenidos en el registro de la tabla de peticiones de tarjetas) y lo enviará al servicio de procesado de lotes de la CA Subordinada (se suspenderán inmediatamente los 3 certificados del usuario).

d) Modificará el registro cambiando su estado a *Suspendida.*

4.9.15.2 Procedimiento de suspensión de la tarjeta de un usuario en la AR del centro

1 Un operador con los permisos adecuados iniciará sesión en la aplicación de administración de la AR del centro.

2 El operador de la AR ordenará a ésta la suspensión de cualquier tarjeta solicitada con el estado *Finalizada con éxito* (seleccionará los datos del correspondiente registro de la tabla de peticiones de tarjeta de la AR).

3 La AR suspenderá la tarjeta usando el mismo procedimiento que realiza el servicio de la AR (paso *4* del procedimiento de suspensión de la tarjeta de un usuario a través de la aplicación GESUSER, página *33*), mostrando por pantalla el resultado de la operación (contenido de la respuesta XML del servicio).

4.9.16 Periodo máximo de suspensión

Un certificado una vez suspendido, podrá permanecer en dicho estado hasta el momento de su expiración.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características de operación de los servicios

Los elementos que sustentan los servicios para albergar las listas de certificados revocados son dos:

- Repositorio Corporativo LDAP del SESCAM
- Repositorio WEB del SESCAM

4.10.2 Disponibilidad de los servicios

Los servicios de descarga de Listas de Certificados Revocados del SESCAM funcionan 24 horas al día, 7 días a la semanas, 365 días al año. El SESCAM dispone de un CPD (Centro de Proceso de Datos) donde dichos repositorios se encuentran situados y monitorizados de forma continua.

4.10.3 Otras funciones de los servicios

Sin estipulación adicional.

4.11 Finalización de la suscripción

La finalización de la suscripción vendrá determinada por la finalización de la relación entre el suscriptor y el SESCAM. En caso de que la misma se produzca antes de que los certificados expiren, se procederá a una revocación de los mismos. En el supuesto de que la relación continúe más haya de la vida de los certificados, se procederá a tantas nuevas emisiones como fuere necesario.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

4.12.1.1 Deposito de claves

En el momento de generación de las claves privadas correspondientes al certificados adscritos a la política de certificación *"Política de EF de Empleado para Cifrado"* con OID 1.3.6.1.4.1.21835.1.1.3.3, éstas son almacenadas por la Autoridad de Salvaguarda de Claves de la Autoridad de Certificación.

Los mecanismos de protección bajo los cuales están custodiadas dichas claves son los propios del producto de Autoridad de Certificación homologado bajo Common Criteria EAL4+ o superior

4.12.1.2 Recuperación de la clave de cifrado de un usuario

Las claves de cifrado de los usuario serán archivadas cifradas (ofuscadas) por la AC Subordinada del SESCAM .

La recuperación del certificado de cifrado de un usuario del SESCAM se podrá realizar remotamente a través de navegadores Web o localmente en la AC Subordinada del SESCAM, por un conjunto n (configurable) de operadores recuperadores de claves, mediante el siguiente procedimiento:

1 El usuario solicitará el inicio de la recuperación de su clave de cifrado a uno de los operadores recuperadores de claves.

2 El operador recuperador de claves iniciará sesión en la aplicación de administración de la CA Subordinada del SESCAM o se conectará con su Navegador Web al servicio de recuperación de claves autenticándose con certificado e iniciará el proceso de recuperación de la clave de cifrado del usuario (identificada por los datos de su certificado).

3 La CA Subordinada generará una contraseña aleatoria y la dividirá en n trozos (contraseña del PKCS# 12 recuperado)

4 Durante el proceso de recuperación, los n trozos permanecerán almacenados en la BD cifrados (ofuscados)

5 La CA Subordinada recuperará la clave privada solicitada y el correspondiente certificado de cifrado y los encapsulará en un PKCS# 12 protegido por la contraseña aleatoria (PKCS# 12 recuperado)

6 La CA Subordinada entregará el PKCS# 12 recuperado y el primer trozo de la contraseña aleatoria que lo protege al operador recuperador de claves y éste se los entregará al usuario

7 El usuario solicitará consecutivamente la continuación de la recuperación de su clave de cifrado a otros n-1 operadores recuperadores de claves.

8 Cada uno de los n-1 operadores recuperadores de claves iniciará sesión en la aplicación de administración de la CA Subordinada del SESCAM o se conectará con su Navegador Web al servicio de recuperación de claves autenticándose con certificado y continuará el proceso de recuperación de la clave de cifrado del usuario (identificada por los datos de su certificado).

9 La CA Subordinada entregará a cada uno de los n-1 operadores recuperadores de claves un trozo distinto de la contraseña aleatoria que protege el PKCS# 12 recuperado

10 Cada entrega quedará registrada en la base de datos de la CA Subordinada, de forma que un mismo operador recuperador de claves no pueda recuperar dos trozos.

11 El usuario recompondrá la contraseña y con ella instalará en su Navegador Web o en una tarjeta su clave privada de cifrado y su correspondiente certificado contenidos en el PKCS# 12 recuperado

Si posteriormente el usuario solicita la recuperación de la misma clave de cifrado, el nuevo PKCS# 12 recuperado y la contraseña que lo protege serán distintos pero su contenido será el mismo (la misma clave y el mismo certificado de cifrado).

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

El SESCAM cuenta con diversas instalaciones físicas en las que alberga sus instalaciones informáticas y desde las que presta los servicios informáticos que le son propios. En esta sección se consideran aquellos elementos de protección física para la prestación de los servicios de gestión de certificados, la custodia de los dispositivos criptográficos y de todos aquellos elementos fundamentales y secundarios de la infraestructura de certificación.

5.1.1 Localización y construcción de las instalaciones

El edificio donde quedan emplazadas las instalaciones informáticas de la infraestructura de clave pública del SESCAM se encuentra situado en un área central y concurrida de la ciudad de Toledo, que garantiza la presencia de fuerzas de seguridad de forma rápida y eficaz en el caso de incidentes, si bien existe personal de seguridad permanentemente emplazado en el edificio.

Los muros perimetrales del edificio están construidos con materiales sólidos, encontrándose todas las puertas y ventanas externas protegidas frente a entradas no autorizadas.

El CDP (Centro de Proceso de Datos) se encuentra aislado físicamente en el edificio del resto de departamentos, únicamente personal autorizado del SESCAM puede acceder a éste.

5.1.2 Acceso físico

El SESCAM mantiene diferentes niveles para el acceso físico a las instalaciones de la infraestructura de clave pública, en primer lugar para el acceso al edificio es requerida la identificación frente a los servicios de vigilancia.

El acceso al Centro de Proceso de Datos únicamente puede ser realizado por personal autorizado, existiendo un control de acceso físico mediante huella dactilar para garantizar que así sea. El acceso de visitas a las instalaciones es siempre supervisado y en acompañamiento de personal autorizado del centro.

También se mantiene un registro de accesos a las áreas restringidas que es archivado de forma segura.

5.1.3 Electricidad y aire acondicionado

Las calidad del suministro eléctrico es garantizado frente a posibles variaciones mediante sistemas de protección ante picos y sobrecargas, caídas de tensión, etc.

El SESCAM dispone a su vez de los mecanismos adecuados para garantizar la continuidad del servicio frente a posibles caídas del suministro eléctrico, incluyendo sistemas de generación autónomos que garantizan la operación de los diferentes sistemas durante el tiempo necesario.

Los sistemas de aire acondicionado dentro del centro de proceso de datos se encuentran redundados, de tal forma que se garantiza las condiciones de temperatura y humedad para el correcto funcionamiento de los equipos informáticos durante la caída y consecuente reparación de uno de ellos.

5.1.4 Exposición al agua

La localización del CPD se encuentra en un lugar alejado de posibles inundaciones dentro del propio edificio. Además existen los servicios de detección adecuadas para detectar una posible exposición de los equipos que componen el sistema.

5.1.5 Prevención y protección de incendios

En general todas las dependencias del SESCAM requieren de sistemas de detección y protección contra incendios tal y como marca la legislación vigente al respecto.

En concreto, las instalaciones donde se ubican los sistemas correspondientes al sistema de gestión de certificados del SESCAM, cuentan además con sistemas específicos de detección, protección y extinción, propios de un centro de procesos de datos.

5.1.6 Almacenamiento de soportes

El almacenamiento de las copias de seguridad de los sistemas es realizado de forma segura en primera instancia dentro de las dependencias del propio centro de proceso de datos en armario ignifugo, y en segunda estancia en un centro externo separado geográficamente que garantiza la recuperación del sistema frente a desastres.

Tanto la gestión de las generación de copias como los procedimientos de recuperación exigen roles diferentes.

5.1.7 Tratamiento de residuos

EL SESCAM, para la eliminación de soportes de respaldo de información exige la destrucción física de la misma, tanto en formato magnético como en papel, de tal forma que la recuperación contenida en estos soportes no sea posible.

5.1.8 Copia de seguridad externa a las instalaciones

El SESCAM mantiene un centro secundario para el proceso de datos, este centro qué actúa como centro de respaldo alberga también copias de seguridad. Los procedimientos de almacenamiento y recuperación de las copias de respaldo del centro primario son de aplicación en este.

5.2 Controles de procedimientos

5.2.1 Perfiles de confianza

La operación de un sistema de confianza requiere que éste sea operado de forma segura y fiable, para ello es necesaria que las diferentes operaciones que se han de realizar sobre el sistema sean realizadas por un perfil determinado. El establecimiento del conjunto de perfiles requeridos para la correcta operación conlleva en primera instancia que el componente tecnológico sobre la que la infraestructura se sustenta permita dicha diferenciación.

El SESCAM utiliza de forma general los perfiles definidos en la norma CEN CWA 14167-1, si bien éstos se han extendidos a las necesidades propias del SESCAM.

El conjunto de Perfiles requeridos por el SESCAM son:

Perfil	Descripción
Oficial de Seguridad	Responsable de la administración e implantación de las políticas y prácticas de seguridad.
Administrador del Sistema	Está autorizado a instalar, configurar y mantener el sistema, con acceso controlado a los aspectos de configuración de seguridad.
Operador del Sistema	Responsable de la operación diaria del sistema, con autorización para llevar a cabo las copias de seguridad y las recuperaciones del sistema.
Auditor del Sistema	Autorizado a acceder en modo lectura a archivos y registros de auditoría del sistema.

Oficial de Registro	Responsable de verificar y aprobar la generación/revocación y suspensión de certificados de entidad final (usuarios).
VIPS	Responsables de la generación de claves y certificado de la Autoridad de Certificación Raíz, asi como del establecimiento de los permisos de uso ésta.

5.2.2 Número de personas por tarea

La correcta operación de ciertas funciones dentro del sistema exige que existan un número de personas autorizadas de forma concurrente para que puedan ser realizadas.

Entre dichas funciones se encuentran todas aquellas realizadas sobre la Autoridad de Certificación Raíz, exceptuando las propias de operación (levantamiento y caída) y auditoría del sistema.

5.2.3 Identificación y autenticación para cada perfil

La identificación de cada perfil frente al sistema es realizado mediante tarjetas inteligentes con claves criptográficas de 1024 bits, el proceso de entrada al sistema exigirá tantas identificaciones de personas como hayan sido definidas para el perfil pretendido.

5.2.4 Perfiles que requieren separación de tareas

La incompatibilidad de funciones de cada perfil es la preestablecida por la normativa europea CEN CWA 14167-1 para sistemas de confianza. Dicha incompatibilidad es de aplicación para todo el sistema de producción del la infraestructura de clave pública del SESCAM, empero la Autoridad de Certificación raíz, donde la funcionalidad del perfil "oficial de seguridad" es dividido en dos subgrupos incompatibles entre si.

5.3 Controles de personal

5.3.1 Requerimientos de historial, calificaciones, experiencia y autorización

El personal responsable de la operación de los servicios de certificación, firma digital y procedimientos de seguridad se encuentra debidamente capacitado y cualificado en dichas áreas.

Los puestos asociados a perfiles de confianza específica se encuentran libres de intereses de carácter personal ajenos al desarrollo normal de la actividad que prestan. Así mismo, para aquellas tareas consideradas

sensibles existe un procedimiento que exige la presencia de un número mínimo y preestablecido de personal cualificado y confiable.

SESCAM no establece requerimientos adicionales respecto al historial del personal involucrado en las operaciones de la infraestructura distintos de los requeridos en cualquiera de los puestos del "Área de Tecnologías de la Información", bajo el cuál opera. La calificación para ejercer los puestos específicos podrá ser obtenida por personal del SESCAM mediante la formación correspondiente.

5.3.2 Procedimientos de revisión de historial

El SESCAM no asignará un perfil de confianza para la gestión u operación del sistema a personal ajeno a la institución, se requiere que toda persona de confianza sea empleado público de la Junta de Comunidades de Castilla la Mancha y estar adscrito como personal del SESCAM. De esta forma queda garantizada la adecuada revisión del historial.

5.3.3 Requerimientos de formación

La Junta de Comunidades de Castilla la Mancha mantiene un plan de formación continuado, el SESCAM como institución perteneciente a la misma hace uso del mismo.

5.3.4 Requerimientos y frecuencia de actualización formativa

Todo el personal que hace uso de los sistemas de certificación y registro de la infraestructura de clave pública requiere de formación previa a su uso. La actualización de la formación se llevará a cabo cada vez que los cambios en los procedimientos o la tecnología utilizada lo requieran.

5.3.5 Secuencia y frecuencia de rotación laboral

No es de aplicación.

5.3.6 Sanciones para acciones no autorizadas

Para el personal funcionario del SESCAM, el determinado por el "Reglamento de Régimen Disciplinario de Funcionarios de la Administración General del Estado", establecido en el Real Decreto 33/1986.

5.3.7 Requerimientos de contratación de personal externo

La contratación de personal sigue los mismos principios establecidos para la contratación de personal de la Junta de Comunidades de Castilla la Mancha, en este sentido es de aplicación lo establecido en:

- Ley 1/2002, de 7 de febrero, por la que se modifica la Ley 3/1988, de 13 de diciembre, de Ordenación de la Función Pública de la Junta de Comunidades de Castilla-La Mancha
- Estatuto de Autonomía de Castilla-La Mancha
- Ley 3/1988, de 1 de diciembre, de Ordenación de la Función Pública de la Junta de Comunidades de Castilla-La Mancha

5.3.8 Documentación suministrada al personal

El personal adscrito al servicio de la infraestructura de clave pública tendrá acceso a toda la información pública de la misma. Se otorgará acceso a la información privada únicamente a aquellos perfiles que por el tipo de tarea que realizan requieran tener detalles de diseño u operación de elementos específicos.

5.4 Procedimientos de auditoría de seguridad

Para auditar los eventos significativos realizados en el ámbito de la infraestructura de clave pública del SESCAM se utilizará la información contenida en la base de datos de logs de la Autoridad de Certificación.

5.4.1 Tipos de evento

Los tipos de eventos registrados en los logs de la Infraestructura de Clave Pública:

- Operaciones realizadas por los diferentes perfiles de la Autoridad de Certificación, incluyendo:
- Cambio en las políticas de certificados.
- Cambio de usuarios
- Cambio en los perfiles de los usuarios
- Cambio en las claves de la Autoridad
- Operaciones realizadas por los operadores de las Entidades de Registro.
- Eventos relativos al ciclo de vida de los certificados.

- Arranque y parada de los sistemas.
- Registro de accesos e intentos de accesos no autorizados.
- Logs de uso de los dispositivos criptográficos hardware

Todos los eventos incluyen los siguientes datos: categoría, fecha, autor, perfil, tipo evento, id evento, módulo, nivel y observaciones.

De forma manual se llevará a cabo una bitácora de la Infraestructura de clave pública donde serán anotadas todas aquellas eventualidades que afecten a la confianza de la misma, como por ejemplo: ceremonia raíz, registro de visitas, informes de intrusión, etc.

5.4.2 Frecuencia del tratamiento de registros de auditoría

Los logs de eventos son revisados al menos de forma semanal por los auditores del SESCAM.

5.4.3 Periodo de conservación de los ficheros de auditoría

Los logs de eventos se mantienen en la base de datos durante toda la vida de la Autoridad de Certificación.

5.4.4 Protección de los ficheros de auditoría

Los ficheros de auditoría generados por la autoridad de certificación y la autoridad de registro son protegidos frente a accesos externos mediante mecanismos de control de acceso lógico. La integridad de la información de dichos ficheros queda garantizada mediante la firma electrónica encadenada de los eventos registrados.

Para el control de ficheros físicos se establecen las adecuadas medidas de seguridad física que impiden su acceso no autorizado.

5.4.5 Procedimiento de copia de seguridad

La copia de seguridad de la base de datos de eventos del sistema se realiza con la misma planificación y controles que para el resto de elementos del sistema de certificación.

5.4.6 Localización del sistema de almacenamiento de registros de auditoría

El almacenamiento de las copias de respaldo de los registros de auditoría es el mismo que el del resto del sistema de certificación.

5.4.7 Notificación del evento de auditoría al causante

Sin estipulación adicional.

5.4.8 Análisis de vulnerabilidad

Los eventos de auditoría registrados son utilizados para verificar posibles vulneraciones al sistema. De forma periódica el SESCAM realiza una comprobación de la integridad de los ficheros de auditoría para constatar que no se han producido vulneraciones al sistema, en el caso de encontrar incidencias o discrepancias se realiza un estudio de las mismas para dilucidar la causa y gravedad de la misma.

5.5 Archivado de información

5.5.1 Tipos de evento y datos registrados

Los tipos de eventos registrados en el archivo son:

- Datos relacionados con el proceso de registro y solicitud de certificados.
- Logs de auditoría de la sección 5.4.1 Tipos de evento.
- Certificados y Listas de Revocación.
- Eventos de error en los procesos realizados.
- En general es registrada toda información concerniente a la gestión de la infraestructura de clave pública y al ciclo de vida de los certificados emitidos por ésta.

5.5.2 Periodo de conservación del archivo de eventos

El archivo de eventos se conserva durante al menos 15 años, desde el momento en que dicho evento se produce.

5.5.3 Protección del archivo de eventos

Los mismos que los declarados para "5.4.4 Protección de los ficheros de auditoría"

5.5.4 Procedimiento de copia de seguridad del archivo de eventos

La copia de seguridad del archivo de eventos del sistema se realiza con la misma planificación y controles que para el resto de elementos del sistema de certificación.

5.5.5 Requerimientos de sellado de tiempo de eventos

La información generada por el SESCAM se almacena con la hora y fecha en la que se produce, no resulta necesario un sello de tiempo que lo garantice, dado que el propio SESCAM se erige como entidad confiable.

5.5.6 Localización del sistema de archivo

El almacenamiento de las copias de respaldo de los registros de auditoría es el mismo que el del resto del sistema de certificación.

5.5.7 Procedimientos de obtención y verificación de información de archivo

La obtención y verificación de la información únicamente puede ser realizada por personal autorizado por el SESCAM para tal fin y siempre bajo autorización previa documentada y firmada por el responsable de seguridad de sistemas de información del SESCAM.

5.6 Renovación de claves

Los certificados emitidos por el SESCAM no son renovables.

Para renovar un certificado de entidad final, debido a que haya sido revocado o haya caducado, se deberá solicitar un nuevo certificado.

5.7 Compromiso de claves y recuperación frente a desastres

5.7.1 Procedimiento de gestión de incidencias y compromisos de seguridad

SESCAM establece los procedimientos para la gestión de incidencias y compromisos de seguridad dentro del marco de su "*Plan frente a contingencias*".

5.7.2 Corrupción de recursos, aplicaciones o datos

SESCAM ha dividido el conjunto de recursos, aplicaciones y datos en diferentes niveles para los cuales ha establecido unas medidas diferentes en el caso de que los mismos se vean corrompidos, a saber:

- ***Autoridad de Certificación raíz***, en este caso existe una copia de backup del sistema y de las claves de la misma, así como el procedimiento y el correspondiente manual para su recuperación.
- ***Servicio de Registro***, este sistema no es considerado crítico, el mismo se mantiene distribuido en la organización. La recuperación implica la revocación de la Autoridad de Registro y la generación de una nueva según el procedimiento al uso, existiendo un manual de instalación y puesta en marcha del mismo.
- Los servicios de ***Revocación de Certificado***s y ***Estado de Certificados*** se encuentran redundados en el centro secundario. En caso de corrupción del sistema se procederá a la restauración de los mismos.
- ***Servicio de Emisión de Certificados***, en el caso de que la instalación de la autoridad de certificación sea dañada y no se pueda recuperar mediante las copias de backup del sistema y de sus claves privadas, se procederá a la creación de una nueva CA de producción.

5.7.3 Compromiso de la clave privada de la Entidad

En caso de que la autoridad de certificación de producción se vea comprometida la autoridad de certificación raíz procederá a la revocación inmediata de la misma, publicando y notificando de forma inmediata el suceso al resto de componentes del sistema mediante la generación de la correspondiente LAR (Lista de Autoridades Revocadas.

En caso de compromiso de la clave privada de la CA raíz, queda comprometido el sistema por completo, se generará la notificación inmediata a todos los elementos sostenidos bajo el paraguas de confianza del sistema, suspendiéndose toda actividad de forma cautelar, hasta que se pueda generar un nuevo marco de confianza mediante la generación de un nuevo certificado raíz.

5.7.4 Desastre sobre las instalaciones

En el caso en el que exista un desastre sobre las instalaciones del centro primario, se procederá a la instalación y puesta en marcha de los elementos necesarios en el centro secundario a efectos de garantizar la continuidad de los sistemas.

5.8 Fin de servicio

5.8.1 Autoridad de Certificación

En caso de finalización de servicio de su sistema de certificación, el SESCAM comunicará el fin, por cualquier medio que garantice el envío y la recepción de la notificación, a todos los suscriptores con certificados en vigor con la antelación suficiente.

De cualquier forma el SESCAM mantendrá los registros del sistema de certificación para proporcionar las evidencias requeridas por procedimientos legales futuros al cese.

El SESCAM trasferirá los certificados en los términos previstos por la Ley 59/2003 de 19 de Diciembre.

5.8.2 Autoridad de registro

Sin estipulación adicional.

6 CONTROLES TECNICOS DE SEGURIDAD

6.1 Generación e instalación del par de claves

6.1.1 Generación par de claves

La generación de claves de la Autoridad de Certificación y del Sistema de recuperación de claves exige que existan al menos un número mínimo de personas designadas por el SESCAM con privilegios de acceso a la Autoridad de Certificación.

El proceso de generación de claves de Operadores de la Entidad de Registro será realizado por los mecanismos propios que ofrezca la autoridad de registro. Así mismo, las claves de estos deberán ser generadas en una Tarjeta Criptográfica.

La generación de claves de las Entidades Finales de Personas físicas se llevará a cabo mediante un mecanismo combinado en el que las claves de los certificados de Autenticación y No-Repudio son generados por la Tarjeta criptográfica. Las claves correspondientes al certificado de cifrado son generadas por la Autoridad de Certificación.

La generación de claves de las Entidades Finales de dispositivos y de código será llevada a cabo por los mecanismos propios de los dispositivos y sistemas utilizados.

6.1.2 Entrega del par de claves al suscriptor

Las claves de los operadores de Registro residen en la tarjeta criptográfica y se entregarán junto con la misma.

Las claves de las Entidades Finales de Personas físicas de Autenticación y de No-Repudio residen en la tarjeta criptográfica y se entregarán junto con la misma, las claves de cifrado son inyectadas en la tarjeta criptográfica por la Entidad de Registro.

Las claves de las Entidades Finales de dispositivos y código residen en el mismo dispositivo y por lo tanto no necesitan ser entregadas.

6.1.3 Entrega clave pública al emisor del certificado

Las claves públicas de los operadores de Registro generadas en la tarjeta criptográfica se entregan a la Autoridad de Certificación mediante una petición de certificación en formato PKCS# 10.

Las claves públicas de las Entidades Finales de Personas físicas de Autenticación y de No-Repudio generadas en la tarjeta criptográfica son enviadas a la Autoridad de Certificación mediante una petición de certificación en formato PKCS# 10. La clave pública de cifrado es generada por la Autoridad de Certificación y por lo tanto no necesita ser entregada a ésta.

Las claves de las Entidades Finales de dispositivos generadas por el mismo dispositivo son enviadas a la Autoridad de Certificación mediante una petición de certificación en formato x.509 o PKCS# 10.

6.1.4 Distribución clave publica de la CA

La clave pública de la Autoridad de Certificación no se distribuye, se publica en el Directorio Corporativo del SESCAM y en los diferentes directorios de los dominios Windows del SESCAM tal como ha sido indicado en ***"2.1.1 Publicación de información de la Autoridad de Certificación"***.

6.1.5 Tamaños de claves

El tamaño de las claves RSA será el siguiente:

- 4096 bits para la Autoridad de Certificación raíz.
- 2048 bits para la Autoridad de Certificación Subordinada.
- 1024 bits para los Operadores de registro.
- 1024 bits para las Entidades Finales, ya sea personas físicas o dispositivos.

6.1.6 Generación parámetros de clave pública

Los parámetros de generación de las claves generados por dispositivo hardware criptográfico utilizan las recomendaciones de la norma FIPS 140-1 Nivel 2.

Los parámetros de generación de las claves generadas en tarjeta criptográfica utilizan la recomendación de la norma CEN CWA 14169 CEN y CEN CWA 14170 o equivalente.

6.1.7 Comprobación calidad parámetros de clave pública

Sin estipulación adicional.

6.1.8 Generación claves en Hardware/Software

La generación de las claves se realiza en los siguientes dispositivos Hardware/Software:

- Autoridad de Certificación: en dispositivo criptográfico hardware.
- Operadores de registro: en la propia tarjeta criptográfica
- Entidades Finales (personas físicas): en la propia tarjeta criptográfica las claves de Autenticación y no-repudio y en la Autoridad de Certificación con procedimientos software las de cifrado.
- Entidades Finales (dispositivos y código): en el propio dispositivo con los procedimientos hardware/software que incorporen.

6.1.9 Propósitos de uso de claves

El propósito de uso de los diferentes certificados emitidos por el SESCAM sigue lo establecido en el documento: *"D.3.2.2 SESCAM – Políticas de Certificación"* , bajo el epígrafe *"Comunidad de Aplicación".*

La utilización de una clave se determina mediante la extensión *KeyUsage* y *ExtKeyUsage*, presentes en todos los certificado.

6.2 Protección clave privada

6.2.1 Estándares de módulos criptográficos

La infraestructura de clave pública del SESCAM hace uso de módulos criptográficos hardware certificados FIPS 140-1 Nivel 2.

Las tarjetas criptográficas utilizadas cumplen con los requisitos establecidos en la norma CEN CWA 14169 o equivalente, estando homologados bajo CC EAL 4+ o superior.

6.2.2 Control multi-persona (n de m) de la clave privada

La utilización de la clave privada de la autoridad de certificación raíz requiere 4 de las 6 posibles personas para la generación del certificado raíz, y 2 de las 6 posibles para la generación/revocación de certificados

de Autoridad de Certificación Subordinada, y de 1 de 6 para la generación de la LAR (Lista de Autoridades Revocadas).

6.2.3 Deposito de la clave privada

Únicamente existe deposito de claves para los certificados de Entidad Final de Persona Física destinadas a proveer cifrado, la autoridad de certificación mediante la funcionalidad de salvaguarda de claves es la responsable de la custodia y acceso a las mismas.

6.2.4 Copia de seguridad de la clave privada

Para las Autoridades de Certificación se dispone de dos conjuntos de seis tarjetas de recuperación inicial para el módulo criptográfico, correspondientes a cada una de las Autoridades de Certificación del SESCAM. También, se mantienen seis tarjetas de activación de la clave privada, de las cuales son necesarias dos.

El resto de claves del sistema susceptibles de copia de respaldo reside ofuscada en la Base de Datos del SESCAM, de la cuál se generan las correspondientes copias tal y como se ha descrito en *"5.1.6 Almacenamiento de soportes".*

6.2.5 Archivo de clave privada

El archivo de las copias de seguridad de las claves privadas del sistema de clave pública será realizado por personal estrictamente autorizado, en armario ignifugo y con al menos dos sistemas de control de acceso adicionales. La recuperación de dichas claves requerirá de las autorizaciones oportunas en el momento en que pudieran ser requeridas.

Las claves privadas de cifrado, generadas por la Autoridad de certificación se almacenan ofuscadas en la base de datos de ésta, de forma que solo los administradores designados o los propios suscriptores podrán recuperarlas.

Las medidas de protección de la información custodiada por el Sistema de salvaguardia de claves garantizan que no sea posible la entrega de claves y de su custodia en claro.

6.2.6 Introducción de la clave privada en el modulo criptográfico

Se consideran los siguientes casos:

- Autoridad de Certificación: Las claves privadas quedan almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes. Estas tarjetas son utilizadas para introducir la clave privada en el módulo criptográfico.

- Operadores de registro: la clave privada se genera en la propia tarjeta criptográfica y no hace falta importarla.
- Entidades Finales (personas físicas): la claves privadas de Autenticación y No-repudio se generan en la propia tarjeta criptográfica mientras que la de cifrado es introducida en la tarjeta por la autoridad de registro.
- Entidades Finales (dispositivos): la clave privada se genera en el propio dispositivo y no hace falta importarla.

6.2.7 Almacenamiento de la clave privada en Modulo criptográfico.

Con la excepción de los certificados de cifrado de Entidad Final que son almacenados con posterioridad a su generación en tarjeta criptográfica, el resto de claves privadas asociadas a dispositivo criptográfico son generadas por éstos y no requieren un almacenamiento posterior.

6.2.8 Método de activación de la clave privada

Para la Autoridad de Certificación y el Sistema de recuperación de claves la clave privada es activada por el grupo de oficiales de seguridad correspondiente.

Para los operadores de registro y las entidades finales de tipo persona física, en posesión de una tarjeta criptográfica, las claves privadas se activan con el PIN de la tarjeta misma.

Para los dispositivos las claves privadas son activadas por los correspondientes administradores con contraseñas.

6.2.9 Método de desactivación de la clave privada

Para la Autoridad de Certificación y el Sistema de recuperación de claves la clave privada es desactivada por un administrador finalizando la aplicación.

Para los operadores de registro y las entidades finales de tipo persona física, en posesión de una tarjeta criptográfica, las claves privadas se desactivan extrayendo la tarjeta del lector.

6.2.10 Método de destrucción de la clave privada

Las claves privadas son destruidas de forma que se impida su robo, modificación, divulgación no autorizada o uso no autorizado. En el caso de claves de usuario en soporte tarjeta mediante la destrucción física de ésta. La destrucción de claves de dispositivo o firma de código no son contempladas por está DPC.

6.2.11 Clasificación de los módulos criptográficos

Los dispositivos criptográficos utilizados por las autoridades de certificación están homologados FIPS 140-1 nivel 2.

Los dispositivos de criptográficos software utilizados por las autoridades de registro están homologados CC EAL4+, bajo el PP CIMC.

Las tarjetas inteligentes utilizadas por suscritores de certificados están homologadas CC EAL 4+, y cumplen además lo definido por la norma europea CEN CWA 14169.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

Las claves públicas son almacenadas por la Autoridad de Certificación.

Cada Autoridad de registro almacena las claves públicas que han sido gestionadas por ella.

6.3.2 Periodo de utilización de las claves pública y privada

Corresponde con el periodo de validez de cada certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Las claves privadas asociadas a los certificados de entidades finales de tipo personas físicas asociadas a una tarjeta inteligente requieren para su activación de un PIN. Este PIN es seleccionado por el suscritor en el momento de realizar la correspondiente solicitud, dicho PIN se graba en la tarjeta sustituyendo el PIN por defecto.

La instalación y puesta en marcha de las claves privadas asociada a los certificados de los dispositivos requiere la utilización de una contraseña.

6.4.2 Protección de los datos de activación

Los datos de activación de la Autoridad de Certificación y de las Autoridades de Registro son conocidos sólo por los correspondientes administradores.

Los PINES y contraseñas asociadas a los certificados de entidades finales deben ser memorizados y no almacenados escritos junto con los dispositivos que albergan las claves privadas.

6.4.3 Otros aspectos de los datos de activación

No se definen limitaciones sobre el tiempo de vida de los datos de activación.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de la seguridad informática

Para garantizar la confiabilidad de la infraestructura de clave pública el SESCAM mantiene un conjunto de controles de seguridad sobre los diferentes elementos que lo componen.

El conjunto de controles de seguridad implantados por el SESCAM quedan divididos según:

- Controles Operacionales
    - Mantenimiento de una Política de Seguridad que engloba el Sistema de Clave Pública, esta política contiene detalles particulares de los requerimientos de seguridad y medidas de salvaguarda a implementar y la forma de usarlos correctamente para alcanzar una seguridad adecuada en consonancia con los objetivos de la organización.
    - SESCAM mantiene una estructura organizativa para la seguridad, que sin menos cabo de los roles específicos de seguridad requeridos por la Infraestructura de clave pública, esta formada por:
        - *Comité de Seguimiento*, grupo designado por el Comité de Dirección, responsable del seguimiento de los proyectos y de los contratos establecidos dentro del marco de aplicación definido en el Plan Director.
        - *Responsable de Seguridad*, es la persona encargada de establecer, comunicar y gestionar las políticas, planes y procedimientos de seguridad necesarios para proteger los activos de la organización en función del riesgo asumible y a un coste razonable.
        - *Equipo de Seguridad*, personal especializado que se encarga de poner en marcha y administrar el conjunto de medidas de salvaguarda aprobadas en el Plan de Seguridad, monitorizando la seguridad del

sistema para que se mantenga dentro de los límites establecidos.

- El SESCAM dispone de un plan de contingencia para la recuperación de los equipos y sistemas de clave pública.
- Los sistemas del SESCAM disponen de herramientas que garantizan su protección frente a ataques provocados por virus informáticos o códigos software maliciosos.
- El SESCAM dispone de herramientas de monitorización de sistemas y detección de intrusiones al mismo.
- Todas aquellas tareas sensibles quedan documentadas para su posterioridad auditoría.
- El conjunto de funciones para la operación del sistema de certificación y registro están reguladas por una política de seguridad reflejada en las aplicaciones.

- Controles de Acceso
  - Existen controles de acceso físico basados en huella dactilar de los que se mantiene registro a las dependencias donde se hayan los sistemas de información. Únicamente el personal autorizado puede acceder a estos sistemas.
  - Los diferentes usuarios del sistema de clave pública disponen de una tarjeta inteligente que contiene sus credenciales.
  - Para aquella información gestionada por el SESCAM de carácter personal se establece los procedimientos de consulta, modificación y borrado exigidos por la LOPD.
  - Los niveles de acceso son revisados de forma periodica.
- Identificación y Autenticación
  - La identificación de los usuarios frente a los sistemas de clave pública es realizada mediante tarjeta inteligente.
  - El uso de perfiles de seguridad sensibles exige la entrada concurrente en el sistema por un conjunto de n de m usuarios autorizados.
  - Las conexiones telemáticas entre los diferentes componentes y actores del sistema de clave pública se realiza mediante conexiones seguras autenticadas extremo a extremo, utilizando protocolos como TLS o IPSec, siendo las comunicaciones cifradas.
- Nivel de Seguridad de los productos utilizados, en la medida de las posibilidades para los diferentes productos utilizados por el SESCAM se exigen las correspondientes homologaciones Common Criteria que sean de relevancia de los servicios

soportados por éstos. En concreto los productos para la gestión de la vida de los certificados y aquellos que han de generar y custodiar las claves privadas, es decir, los dispositivos criptográficos, tendrán una homologación CC EAL4+ o superior.

- Disponibilidad de los sistemas, el SESCAM dispone de un centro de proceso de datos secundario donde se encuentran redundados aquellos sistemas y subsistemas críticos para la operativa diaria de la organización.
- Auditoría de la seguridad, de forma regular el SESCAM realiza auditorías de seguridad que incluyen test de penetración a sus sistemas.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de CA (Autoridad "Técnica" de Certificación) y AR (Autoridad "Técnica" de Registro) son fiables, de acuerdo con la especificación técnica CEN CWA 14167-1, evaluándose el grado de cumplimiento mediante un perfil de protección adecuado, de acuerdo con la norma CIMC. Igualmente, dichas aplicaciones se encuentran homologadas por el CCN (Centro Criptológico Nacional).

De forma periódica se evalúan las características (vulnerabilidades, riesgos y costes de los mecanismos de seguridad implantados o a implantar) para la arquitectura tecnológica establecida. Dicha evaluación se entrega al Comité de Seguimiento para su valoración.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Los servicios de seguridad soportados por una Infraestructura de Clave Pública (PKI) constituyen la herramienta principal a la hora de garantizar la autoría, la integridad, la confidencialidad y el no repudio en una gran variedad de eventos en aplicaciones del SESCAM basadas en Internet/Intranet, como el control de acceso, correo seguro o el gobierno electrónico.

Las entidades finales que van a hacer uso de las funcionalidades y servicios proporcionados por la infraestructura de clave pública del SESCAM, principalmente empleados, a través de sus aplicaciones de cliente y, servidores de aplicaciones o aplicaciones en general, harán uso de la tecnología de clave pública para múltiples propósitos: identificación y autenticación, control de acceso, firma digital, cifrado, etc.

El SESCAM vigila que dichas aplicaciones que hacen uso de los servicios ofrecidos por su infraestructura cumplan con los requerimientos y las premisas establecidas en esta DPC para el uso de los mismos, introduciendo los controles pertinentes en su metodología de desarrollo software y de implantación de sistemas.

6.6.2 Controles de gestión de seguridad

El SESCAM mantiene establecido el siguiente conjunto de controles para la correcta gestión de la seguridad:

- Comprobación de la integridad de los sistemas de Bases de Datos utilizados por los sistemas de Certificación.
- Comprobación de correcto funcionamiento de los sistemas.
- Comprobación periódica de configuraciones de seguridad de los diferentes elementos, tales cómo: bases de datos, sistemas operativos, componentes de red, directorios LDAP, etc.

Además, se mantiene actualizado el plan de sistemas de la infraestructura de clave pública mediante una detección temprana de necesidades funcionales y organizativas del SESCAM que requieran del uso de la infraestructura.

6.6.3 Evaluación del nivel de seguridad del ciclo de vida

De forma periódica se evalúan las características (vulnerabilidades y riesgos de los mecanismos de seguridad implantados) para la arquitectura tecnológica establecida. Dicha evaluación se entrega al Comité de Seguimiento para su valoración.

6.7 Controles de seguridad de la red

El SESCAM garantiza el correcto uso y acceso de los sistemas que conforman su infraestructura de clave pública mediante el siguiente conjunto de controles de seguridad de red implantados en sus sistemas:

- Cortafuegos para proteger la red interna frente a accesos externos no autorizados. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación del sistema, actuando como primera barrera de seguridad perimetral.
- Medidas anti-spoofing y frente ataques de denegación de servicio.
- Uso de protocolos seguros, confidenciales y autenticados, entre los elementos que conforman la infraestructura de clave pública.
- Mantenimiento en alta disponibilidad mediante clusterización de routers y firewalls.
- Mantenimiento de centro de respaldo que garantiza la continuidad de los servicios de red críticos del SESCAM.

- Controles de acceso físico y lógico a los diferentes dispositivos de red.
- Monitorización de estado de los diferentes elementos de la red.

6.8 Sello de Tiempo

No aplicable.

7 PERFILES DE CERTIFICADOS Y LISTAS DE REVOCACION

7.1 Perfil de certificados

Esta sección se encuentra públicamente disponible en el documento "D.3.2.2 SESCAM – Políticas de Certificación.pdf", que puede encontrarse en la dirección web http://sescam.jccm.es/pki/dpc/pc.pdf.

7.2 Perfil de Listas de Revocación

Esta sección se encuentra públicamente disponible en el documento *"D.3.2.2 SESCAM – Políticas de Certificación.pdf",* que puede encontrarse en la dirección web http://sescam.jccm.es/pki/dpc/pc.pdf.

8 Auditoría de conformidad

El SESCAM verificará la conformidad de que el sistema de clave pública que mantiene y explota cumple con los requisitos procedimentales, técnicos, operacionales y de seguridad necesarios para la prestación de los servicios de certificación que provee.

La ejecución de las auditorías de conformidad podrán ser llevadas por personal interno del SESCAM, si bien podrá delegarse a una entidad externa.

8.1 Frecuencia de la auditoría de conformidad

La frecuencia de auditorías de conformidad es realizada de forma periódica, las mismas serán planificadas según los requerimientos y necesidades operaciones del sistema, así como del conjunto de actividades objeto de la auditoría.

El tipo de auditorías podrá ser en todo caso parcial sobre elementos o funciones concretas del sistema.

8.2 Identificación y calificación del auditor

Los procesos de auditoría podrán ser realizados por el "Personal de Seguridad" del SESCAM.

EL SESCAM exigirá la independencia y experiencia contrastada en Sistemas de Clave Pública en los procesos de contratación o delegación de auditorías a entidades externas.

8.3 Relación del auditor con la entidad auditada

El SESCAM podrá emplear auditores internos o externos siempre y cuándo los mismos sean funcionalmente independientes del sistema o servicio objeto de auditoría.

8.4 Relación de elementos objeto de auditoría

Los elementos objeto de auditoría en el marco de esta DPC son los siguientes:

- Ceremonia de la Autoridad de Certificación Raíz.
- Procesos relacionados con la gestión propia de los servicios de gestión de certificados llevados a cabo por la Autoridad de Certificación.
- Proceso relacionados con los procedimientos de registro de suscriptores.
- Sistemas de Información.
- Seguridad de los Centros de Procesos de Datos
- Aplicaciones corporativas del SESCAM que hacen uso de los certificados.
- Documentación

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez se haya detectado una no-conformidad por la auditoría se procederá a establecer un plan de acciones correctivas para subsanar la posible deficiencia, con posterioridad se verificará que las acciones planificadas han resuelto adecuadamente la no-conformidad.

En caso de que existan no-conformidades que no puedan ser resueltas y que afecten a la seguridad, integridad, confiabilidad o continuidad de los servicios se procederá según el Plan de Contigencia.

8.6 Tratamiento de los informes de auditoría

Los informes de auditoría serán entregados al Comité de Seguridad y al Responsable de seguridad del SESCAM para su evaluación.

9 Requisitos comerciales y legales

9.1 Tarifas

El uso de los servicios prestados por el SESCAM no estipula una tarifa para sus suscriptores.

9.2 Capacidad Financiera

Todos y cada uno de los certificados emitidos en el ámbito del SESCAM bajo las Políticas de Certificación definidas no admiten ninguna responsabilidad económica que se pudiera derivar del uso de los mismos.

El SESCAM establece asimismo las relaciones jurídicas y contractuales que vinculan a los suscriptores y verificadores en caso de infracción de sus obligaciones o de la legislación aplicable.

9.2.1 Seguro de responsabilidad civil

Sin estipulación adicional.

9.2.2 Otros activos

Sin estipulación adicional.

9.2.3 Cobertura de aseguramiento para suscriptores y terceros que confíen en certificados

Sin estipulación adicional.

9.3 Confidencialidad

9.3.1 Información confidencial

Para prestar los servicios de certificación la Autoridad de Certificación y las Autoridades de Registro necesitan obtener información de carácter personal y por lo tanto esta información tiene que gestionarse de acuerdo con la legislación de protección de datos.

La información de carácter personal gestionada por el SESCAM es la obtenida durante el proceso de registro y la incluida en el certificado:

- Solicitudes de certificado, aprobadas o denegadas.
- Datos personales requeridos y utilizados durante el proceso de registro.
- Registro de transacciones.
- Plan de seguridad de sistemas y de continuidad de negocio y de emergencia.
- Toda información clasificada como "Confidencial".

La Infraestructura de Clave Pública de SESCAM en el tratamiento de los datos personales que precisa se sujeta a lo dispuesto en la Ley Orgánica 15/99 de 13 de diciembre, de Protección de datos de carácter personal y a las disposiciones dictadas en su desarrollo, la Ley Orgánica 53/2003 de 19 de Diciembre, sobre firma electrónica.

El SESCAM adoptará las medidas necesarias para evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta en todo momento del estado de la tecnología, de acuerdo con lo previsto en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

En todo caso los datos de carácter personal utilizados tienen la calificación de nivel básico para el tratamiento de los mismos según LOPD.

9.3.2 Información no confidencial

La información indicada a continuación no es considerada de carácter confidencial:

- Certificados emitidos y sus estados.
- Nombre, apellidos y dirección de correo del suscriptor del certificado.
- Las listas de revocación (LCR).

- La declaración de practicas de certificación (DPC) y las políticas de certificación (PC)
- Toda información no clasificada como "Confidencial" y no incluida en la sección 9.3.1 Información confidencial de esta DPC.

9.3.3 Responsabilidad para la protección de información confidencial

EL SESCAM es responsable de la correcta protección de la información calificada como confidencial, para lo que adopta y establece los mecanismos adecuados que así lo garantizan.

9.4 Protección de datos personales

9.4.1 Plan de Protección de Datos Personales

EL SESCAM mantiene un plan de protección de datos personales según lo establecido en la Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal.

9.4.2 Información considerada privada

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

La siguiente información propia de cada suscriptor es considerada privada:

- Claves privadas de suscriptores generadas o salvaguardadas por la Autoridad de Certificación.
- Información de carácter personal incluida en la solicitud de certificado.

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 privada

No se considera información privada de carácter personal aquella que es incluida en el certificado expedido al suscriptor, tampoco aquella

información que permita a los verificadores validar el estado del certificado de un suscriptor.

La información de carácter personal incluida en los certificados es recabada durante la solicitud de los mismos, advirtiendo al suscriptor en los mismo términos que la ley de firma electrónica 53/2003 prevé.

9.4.4 Responsabilidad correspondiente a la protección de los datos personales

El SESCAM es responsable último de la correcta protección de los datos de carácter personal, para ello garantiza el cumplimiento de sus obligaciones legales.

9.4.5 Prestación del consentimiento en el uso de los datos personales

La infraestructura de Certificación del SESCAM no requiere del consentimiento expreso para el uso de los datos personales, por estar estos ya a disposición del SESCAM.

En cualquier caso, el SESCAM en el proceso de solicitud y durante el acto de activación de claves recaba el consentimiento, sin necesidad de que éste tenga que ser expreso, por parte del suscriptor para su incorporación en los certificados digitales que le son entregados.

9.4.6 Divulgación de la información originada por procedimientos administrativos y/o judiciales

EL SESCAM está obligada a revelar la identidad de los firmantes a requerimiento de los órganos judiciales en el ejercicio de las funciones que tengan atribuidas y resto de supuestos previstos en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre ,de la Protección de Datos de Carácter Personal donde fuere requerido.

Los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, administrativo o disciplinario si correspondiera, incluso sin consentimiento del suscriptor del certificado.

9.4.7 Otros supuestos de divulgación de la información

No han sido contemplados otros supuestos de divulgación adicionales.

9.5 Derechos de propiedad intelectual

El SESCAM es la entidad que mantiene los derechos de propiedad intelectual sobre la Declaración de Practicas de Certificación y de las diferentes Políticas de Certificado que gobiernan el ciclo de vida de éstos. Igualmente SESCAM es el propietario en exclusiva de los certificados y listas de revocación que emite.

La propiedad exclusiva de las claves generadas corresponde a sus suscriptores, al igual que los nombres relativos a éstos y que le son propios. Así mismo el suscriptor mantiene el derecho sobre nombre distinguido que aparece en el certificado y que le identifica.

Los OID utilizados por esta DPC y por cada Política de Certificado para su nombramiento único son propiedad del SESCAM, quién se ha registrado en la IANA (Internet Assigned Number Authority) bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1.IANA-Registered Private Enterprises), habiendo asignado ésta al SESCAM el identificador de objetos ***1.3.6.1.4.1. 21835***.

La gestión y uso de este OID es exclusiva del SESCAM no pudiendo ser utilizado en forma alguna por terceras partes excepto para el uso que se describe para cada uno de los especificados en esta DPC y en las correspondientes Políticas de Certificación.

9.6 Obligaciones y Responsabilidad Patrimonial

La autoridad de Certificación del SESCAM es responsabilidad de la Administración, la cuál se asienta sobre bases objetivas y cubre toda lesión que los particulares sufran siempre que sea consecuencia del funcionamiento normal o anormal de los servicios públicos.

9.6.1 Obligaciones de la Autoridad de Certificación

El SESCAM cuando actúa como Autoridad de Certificación bajo las directivas definidas en esta DPC asume las siguientes obligaciones:

- Emitir los certificados solicitados en cumplimiento de las normas y procedimientos establecidos en esta DPC, en las políticas de certificación (PC) y en las leyes vigentes.
- Cumplir con los requerimientos de seguridad física, de procedimientos, personales y técnicos definidos en su plan de seguridad.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación prestados.
- Emplear personal cualificado y debidamente formado en los procesos a realizar para la prestación del servicio ofrecido.

- Emitir los certificados en cumplimiento del estándar X.509 y de los requerimientos de la petición.

- Publicar las políticas de certificación y esta DPC en la ubicación indicada en las PCs.

- Revocar / Suspender los certificados siguiendo los procedimientos descritos en la sección 4.3 y publicar la nueva LCR en la ubicación indicada el las Políticas de Certificación.
- Mantener un registro con la información relativa a los certificados emitidos que pueda ser consultado solamente por personal autorizado.
- Cumplir con todos los requerimientos de la normativa sobre protección de datos de carácter personal.
- Archivar las claves de los certificados de cifrado de forma segura.

9.6.2 Obligaciones de la Autoridad de Registro

La autoridad de registro asume las siguientes obligaciones:

- Comprobar la identidad y los datos del solicitante y del suscriptor conforme a los procedimientos establecidos en esta DPC y el las Políticas de Certificación especificas de cada tipo de certificado.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación prestados.
- Emplear personal cualificado y debidamente formado en los procesos a realizar para la prestación del servicio ofrecido.
- Enviar las peticiones de certificación en cumplimiento del estándar X.509.
- Gestionar los procedimientos de suspensión / revocación y renovación de certificados según los procedimientos descritos en la sección 4.3.

9.6.3 Obligaciones de los suscriptores

El solicitante del certificado está obligado a:

- Garantizar que toda la información aportada durante el proceso de registro de la petición del certificado es cierta y correcta.

- Solicitar el certificado siguiendo el procedimiento definido en la sección 4.1 Solicitud de certificados.

El suscriptor del certificado está obligado a:

- Aceptar las directivas establecidos en esta DPC y en las Políticas de Certificación.

- Notificar inmediatamente a la Autoridad de Registro de cualquier información incorrecta que haya sido incluida en el certificado.

- Custodiar de forma diligente los certificados, las claves, el soporte de las mismas y los códigos de activación.

- Notificar inmediatamente a la Autoridad de registro la pérdida, el robo o cualquier compromiso potencial de sus claves privadas.
- Solicitar la Suspensión / Revocación de los certificados cuando se den las condiciones descritas en la sección 4.3 y según los procedimientos allí definidos.
- Aceptar que sus certificados sean publicados en un repositorio común y público.
- Utilizar los certificados adecuadamente y para los usos especificados en esta DPC y en las Políticas de certificación específicas.
- La responsabilidad derivada del uso de los certificados pertenecientes a esta infraestructura de clave pública vendrá en todo caso impuesta por el reglamento disciplinario de aplicación en el ámbito del SESCAM para los certificados de persona física empleado del SESCAM.

9.6.4 Obligaciones de terceras partes verificadoras

Las terceras partes que confiarán en los certificados están obligadas a:

- Cumplir con la legislación vigente aplicable al uso de los certificados.
- Obtener y verificar todos los certificados de la cadena de confianza antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Verificar la validez de los certificados a través de las Listas de Revocación obtenidas con una frecuencia no superior a 24 horas.
- No comprometer de forma intencionada o por negligencia la seguridad de los servicios de certificación.

9.6.5 Obligaciones de otros participantes

Sin estipulación adicional.

9.7 Renuncias de garantías

La infraestructura de clave pública del SESCAM podrá renunciar a todas las garantías del servicio que presta y que no se encuentren vinculadas a las obligaciones establecidas por la Ley 53/2003 de firma electrónica.

9.8 Limitaciones de responsabilidad

El SESCAM sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo. No responderá cuando el firmante supere los límites que figuran en la política del certificado en cuanto a sus posibles usos y no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante. Tampoco responderá el SESCAM si el destinatario de los documentos firmados electrónicamente no comprueba y tiene en cuenta las restricciones que figuran en éste en cuanto a sus posibles usos.

El SESCAM no establece ningún valor máximo de las transacciones comerciales que puedan realizarse con los certificados, dado que este uso queda excluido en el entorno corporativo. Para aquellos certificados que pueda emitir el SESCAM con esta funcionalidad se consignará, además de en la política de certificación, en el certificado de forma clara el limite de las transacciones por las que SESCAM acepta responsabilidad.

9.9 Indemnizaciones

No se establecen cláusulas de indemnidad de los suscriptores ni de los verificadores.

9.10 Plazo y finalización

9.10.1 Plazo

El plazo de vigencia de la presente DPC y sus Políticas de Certificación asociadas corresponde al tiempo durante el que permanece existiendo una relación con los suscriptores y verificadores que hacen uso de los certificados vigentes emitidos bajo esta DPC.

9.10.2 Finalización

La finalización de aplicabilidad de la presente DPC y sus políticas de certificación vendrá determinada bien por finalización de servicio, bien por la publicación de una nueva DPC según lo establecido en 9.12 Modificaciones.

9.10.3 Efectos de finalización y supervivencia

El SESCAM vigilará al menos los requisitos contenidos en las secciones Obligaciones, Responsabilidad civil, Auditoría de conformidad y Confidencialidad, continúen vigentes después de la finalización de la

DPC y de los diferentes instrumentos jurídicos que vinculen la Autoridad de Certificación del SESCAM con suscriptores y verificadores.

9.11 Notificaciones

Los suscriptores y verificadores de certificados de entidad final, correspondientes a las clases 3, 4 y 5 deberán notificar a los responsables de las Autoridades Registro cualquier suceso que afecte a la seguridad de sus claves o a la continuidad de su relación con el SESCAM. Dichas comunicaciones deberán realizarse bien mediante el envío de un correo electrónico al servicio de registro de la entidad que gestiono la solicitud o bien de forma presencial.

No se establecen procedimientos particulares para otras notificaciones entre participes de la PKI, cuándo sea necesario la notificación podrá realizarse de la forma más ágil y efectiva posible, siempre y cuándo quede traza de la misma.

9.12 Modificaciones

9.12.1 Procedimiento para modificaciones

El SESCAM podrá modificar esta declaración de prácticas de certificación (DPC) y sus políticas de certificación (PC).

Los cambios aportados deberán garantizar el mantenimiento del nivel de calidad exigido y tendrán que ser justificados desde el punto de vista legal, técnico y procedimental.

Se establece un sistema de numeración para el mantenimiento de las versiones y el numero de versión se añadirá al nombre de la DPC ("DPC del SESCAM Versión 1") como indicado en la sección 1.2 Identificación.

9.12.2 Periodo y mecanismos para notificaciones

La entrada en vigor de una nueva DPC se comunicará a los suscriptores a través del deposito *"2.1 Repositorios"* con una antelación de 30 días. Pasados los 30 días se podrá retirar la referencia al cambio y la nueva DPC entrará en vigor.

9.12.3 Circunstancias en las que un OID tiene que ser cambiado

No estipulado.

9.13 Resolución de conflictos

En caso de existir disputas relacionadas con los servicios o disposiciones contempladas por esta Declaración de Prácticas de Certificación, las partes se someterán a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa.

9.14 Legislación aplicable

No se considera ley de aplicación pues se trata de una infraestructura de carácter corporativo en un entorno en el que el tratamiento de la información es de carácter "interna" y la información, por tanto, se considera reservada.

9.15 Conformidad con la ley aplicable

Si bien los procedimientos se han establecido conforme a la Ley 53/2003 de Firma Electrónica, en caso de disputa se aplicará el régimen de disciplina interna del SESCAM para la resolución de incidencias y/o disputas.

9.16 Cláusulas diversas

9.16.1 Acuerdo íntegro

Ninguno de los términos de esta Declaración de Prácticas de Certificación que afecte directamente a los derechos y obligaciones del SESCAM y que no afecte al resto de las partes, puede ser corregido, renunciado, suplementado, modificado o eliminado si no es mediante documento escrito autenticado del SESCAM.

9.16.2 Subrogación

Los derechos, deberes y obligaciones asociados a las Autoridades de Certificación del SESCAM no podrán ser objeto de cesión a terceros. En el caso de subrogación del servicio, se procederá a la finalización de las Autoridades de Certificación.

9.16.3 Divisibilidad

En el caso que una o mas cláusulas de esta DPC sea o llegase a ser inválida, ilegal, o inexigible legalmente, tal inaplicabilidad no afectará a ninguna otra cláusula, sino que se actuará entonces como si las cláusula o cláusulas inaplicables nunca hubieran sido contenidas por esta DPC, y

en tal grado como sea posible se interpretará la DPC para mantener la voluntad original de la misma.

9.16.4 Fuerza Mayor

En caso de fuerza mayor se atenderá a lo establecido en la cláusula 9.8 Limitaciones de Garantía.

9.17 Otras cláusulas

Sin estipulación adicional.