

# POLÍTICA DE CERTIFICACIÓN



**Camerfirma**

Certificado Digital

## CAMERFIRMA SELLO ELECTRÓNICO

Versión 1.0

Idioma: **Castellano**

Fecha: **Mayo 2016**

Estado del documento: **Activo**

## **Información sobre el documento**

---

<b>Nombre:</b>	Política de Certificación Camerfirma para Sello Electrónico
<b>Código</b>	PC-SELLO
<b>Versión:</b>	1.0
<b>Elaborado por:</b>	AC Camerfirma SA
<b>Idioma:</b>	Castellano
<b>Descripción:</b>	Define los criterios básicos a seguir por la CA que emita este tipo de certificados, por las RA's que pudiera utilizar y por suscriptores/creadores del sello y Partes usuarias de este tipo de certificados.
<b>Fecha de edición:</b>	Mayo 2016
<b>Estado del documento:</b>	Activo
<b>Referencia (OID):</b>	<b>1.3.6.1.4.1.17326.10.16.2</b>
<b>Localización:</b>	<a href="http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/">http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/</a>

---

## **Control de versiones**

<b>VERSIÓN</b>	<b>MOTIVACIÓN DEL CAMBIO</b>	<b>PUBLICACIÓN</b>
1.0	Creación del documento	Mayo 2016

## **Identificación de políticas**

La forma de identificar distintos tipos de certificados digitales es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta.

El identificador de política está compuesto por una serie de números separados entre sí por puntos y con un significado concreto de cada uno de ellos. Dentro de un mismo tipo de certificados podemos definir diferentes subtipos en función a algunas características especiales. En concreto, para este tipo de certificados distinguimos dentro del tipo genérico de certificados camerales de representante, varios subtipos de certificados en función del soporte de almacenamiento de las claves, así como de la entidad que genera las claves (el propio Suscriptor/creador del sello o el prestador de servicios).

Ver 1.3 Identificación

# Índice de Contenido

<b>1. Introducción</b>	<b>10</b>
<b>1.1. Consideración Inicial</b>	<b>10</b>
<b>1.2. Vista General</b>	<b>10</b>
<b>1.3. Identificación</b>	<b>12</b>
<b>1.4. Comunidad y Ámbito de Aplicación</b>	<b>12</b>
1.4.1 Autoridad de Certificación (AC)	13
1.4.2 Autoridad de Registro (AR)	13
1.4.3 Suscriptor / creador del sello	13
1.4.4 Parte usuaria	13
1.4.5 Solicitante	13
1.4.6 Ámbito de Aplicación y Usos	14
1.4.6.1 Usos Prohibidos y no Autorizados	14
<b>1.5. Contacto</b>	<b>14</b>
<b>2. Cláusulas Generales</b>	<b>15</b>
<b>2.1. Obligaciones</b>	<b>15</b>
2.1.1 AC	15
2.1.2 AR	15
2.1.3 Suscriptor / creador del sello	16
2.1.4 Solicitante	16
2.1.5 Parte usuaria	17
2.1.6 Repositorio.	17
<b>2.2. Responsabilidad</b>	<b>17</b>
2.2.1 Exoneración de responsabilidad	18
2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones	18
<b>2.3. Responsabilidad financiera</b>	<b>18</b>
<b>2.4. Interpretación y ejecución</b>	<b>18</b>
2.4.1 Legislación	18
2.4.2 Independencia	19
2.4.3 Notificación	19
2.4.4 Procedimiento de resolución de disputas	19
<b>2.5. Tarifas</b>	<b>19</b>
2.5.1 Tarifas de emisión de certificados y renovación	19
2.5.2 Tarifas de acceso a los certificados	19
2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados	19
2.5.4 Tarifas por el acceso al contenido de estas Políticas de Certificación	19
2.5.5 Política de reintegros	20
<b>2.6. Publicación y repositorios</b>	<b>20</b>
2.6.1 Publicación de información de la AC	20
2.6.1.1 Políticas y Prácticas de Certificación	20

2.6.1.2	Términos y condiciones _____	20
2.6.1.3	Difusión de los certificados _____	21
2.6.2	Frecuencia de publicación _____	21
2.6.3	Controles de acceso _____	21
<b>2.7.</b>	<b>Auditorias _____</b>	<b>21</b>
2.7.1	Frecuencia de las auditorias _____	21
2.7.2	Identificación y calificación del auditor _____	22
2.7.3	Relación entre el auditor y la AC _____	22
2.7.4	Tópicos cubiertos por la auditoria _____	22
<b>2.8.</b>	<b>Confidencialidad _____</b>	<b>22</b>
2.8.1	Tipo de información a mantener confidencial _____	22
2.8.2	Tipo de información considerada no confidencial _____	22
2.8.3	Divulgación de información de revocación de certificados _____	23
2.8.4	Envío a la Autoridad Competente _____	23
<b>2.9.</b>	<b>Derechos de propiedad intelectual _____</b>	<b>23</b>
<b>3.</b>	<b><i>Identificación y Autenticación</i> _____</b>	<b>24</b>
<b>3.1.</b>	<b>Registro inicial _____</b>	<b>24</b>
3.1.1	Tipos de nombres _____	24
3.1.2	Pseudónimos _____	24
3.1.3	Reglas utilizadas para interpretar varios formatos de nombres _____	24
3.1.4	Unicidad de los nombres _____	24
3.1.5	Procedimiento de resolución de disputas de nombres _____	24
3.1.6	Reconocimiento, autenticación y función de las marcas registradas _____	24
3.1.7	Métodos de prueba de la posesión de la clave privada _____	24
3.1.8	Autenticación de la identidad de una Entidad _____	25
3.1.9	Autorización de la Entidad al Solicitante _____	25
<b>3.2.</b>	<b>Renovación de la clave _____</b>	<b>25</b>
<b>3.3.</b>	<b>Modificación de certificados _____</b>	<b>25</b>
<b>3.4.</b>	<b>Reemisión después de una revocación _____</b>	<b>26</b>
<b>3.5.</b>	<b>Solicitud de revocación _____</b>	<b>26</b>
<b>4.</b>	<b><i>Requerimientos Operacionales</i> _____</b>	<b>27</b>
<b>4.1.</b>	<b>Solicitud de certificados _____</b>	<b>27</b>
<b>4.2.</b>	<b>Petición de certificación cruzada _____</b>	<b>27</b>
<b>4.3.</b>	<b>Emisión de certificados _____</b>	<b>27</b>
<b>4.4.</b>	<b>Aceptación de certificados _____</b>	<b>28</b>
<b>4.5.</b>	<b>Suspensión y revocación de certificados _____</b>	<b>28</b>
4.5.1	Causas de revocación _____	28
4.5.2	Quién puede solicitar la revocación _____	29
4.5.3	Procedimiento de solicitud de revocación _____	29
4.5.4	Periodo de revocación _____	30
4.5.5	Suspensión _____	30
4.5.6	Procedimiento para la solicitud de suspensión _____	30
4.5.7	Límites del periodo de suspensión _____	30
4.5.8	Frecuencia de emisión de CRL's _____	30

4.5.9	Requisitos de comprobación de CRL's _____	31
4.5.10	Disponibilidad de comprobación on-line de la revocación _____	31
4.5.11	Requisitos de la comprobación on-line de la revocación _____	31
4.5.12	Otras formas de divulgación de información de revocación disponibles _____	31
4.5.13	Requisitos de comprobación para otras formas de divulgación de información de revocación _____	31
4.5.14	Requisitos especiales de revocación por compromiso de las claves _____	31
<b>4.6.</b>	<b>Procedimientos de Control de Seguridad _____</b>	<b>32</b>
4.6.1	Tipos de eventos registrados _____	33
4.6.2	Frecuencia de procesado de Logs _____	33
4.6.3	Periodos de retención para los Logs de auditoría _____	33
4.6.4	Protección de los Logs de auditoría _____	34
4.6.5	Procedimientos de backup de los Logs de auditoría _____	34
4.6.6	Sistema de recogida de información de auditoría _____	34
4.6.7	Notificación al sujeto causa del evento _____	34
4.6.8	Análisis de vulnerabilidades _____	34
<b>4.7.</b>	<b>Archivo de registros _____</b>	<b>34</b>
4.7.1	Tipo de archivos registrados _____	34
4.7.2	Periodo de retención para el archivo _____	35
4.7.3	Protección del archivo _____	35
4.7.4	Procedimientos de backup del archivo _____	35
4.7.5	Requerimientos para el sellado de tiempo de los registros _____	35
4.7.6	Sistema de recogida de información de auditoría _____	35
4.7.7	Procedimientos para obtener y verificar información archivada _____	35
<b>4.8.</b>	<b>Cambio de clave de la AC _____</b>	<b>35</b>
<b>4.9.</b>	<b>Recuperación en caso de compromiso de la clave o desastre _____</b>	<b>36</b>
4.9.1	La clave de la AC se compromete _____	36
4.9.2	Instalación de seguridad después de un desastre natural u otro tipo de desastre _____	36
<b>4.10.</b>	<b>Cese de la AC _____</b>	<b>36</b>
<b>5.</b>	<b><i>Controles de Seguridad Física, Procedimental y de Personal _____</i></b>	<b>38</b>
<b>5.1.</b>	<b>Controles de Seguridad física _____</b>	<b>38</b>
5.1.1	Ubicación y construcción _____	39
5.1.2	Acceso físico _____	39
5.1.3	Alimentación eléctrica y aire acondicionado _____	39
5.1.4	Exposición al agua _____	39
5.1.5	Protección y prevención de incendios _____	39
5.1.6	Sistema de almacenamiento. _____	39
5.1.7	Eliminación de residuos _____	39
5.1.8	Backup remoto _____	40
<b>5.2.</b>	<b>Controles procedimentales. _____</b>	<b>40</b>
5.2.1	Roles de confianza _____	40
5.2.2	Número de personas requerido por tarea _____	40
5.2.3	Identificación y autenticación para cada rol _____	41
<b>5.3.</b>	<b>Controles de seguridad de personal _____</b>	<b>41</b>
5.3.1	Requerimientos de antecedentes, calificación, experiencia, y acreditación _____	41

5.3.2	Procedimientos de comprobación de antecedentes _____	42
5.3.3	Requerimientos de formación _____	42
5.3.4	Requerimientos y frecuencia de la actualización de la formación _____	42
5.3.5	Frecuencia y secuencia de rotación de tareas _____	42
5.3.6	Sanciones por acciones no autorizadas _____	42
5.3.7	Requerimientos de contratación de personal _____	42
5.3.8	Documentación proporcionada al personal _____	43
<b>6.</b>	<b><i>Controles de Seguridad Técnica</i></b> _____	<b>44</b>
<b>6.1.</b>	<b>Generación e instalación del par de claves</b> _____	<b>44</b>
6.1.1	Generación del par de claves de la AC _____	44
6.1.2	Generación del par de claves del Suscriptor _____	44
6.1.3	Entrega de la clave privada al Suscriptor _____	44
6.1.4	Entrega de la clave pública del Firmante al emisor del certificado _____	45
6.1.5	Entrega de la clave pública de la CA a los Usuarios _____	45
6.1.6	Tamaño y periodo de validez de las claves del emisor _____	45
6.1.7	Tamaño y periodo de validez de las claves del Suscriptor _____	46
6.1.8	Parámetros de generación de la clave pública _____	46
6.1.9	Comprobación de la calidad de los parámetros _____	46
6.1.10	Hardware / software de generación de claves _____	46
6.1.11	Fines del uso de la clave _____	46
<b>6.2.</b>	<b>Protección de la clave privada</b> _____	<b>46</b>
<b>6.3.</b>	<b>Estándares para los módulos criptográficos</b> _____	<b>47</b>
6.3.1	Control multi-persona (n de entre m) de la clave privada _____	47
6.3.2	Depósito de la clave privada (key escrow) _____	47
6.3.3	Copia de seguridad de la clave privada _____	47
6.3.4	Archivo de la clave privada _____	47
6.3.5	Introducción de la clave privada en el módulo criptográfico _____	48
6.3.6	Método de activación de la clave privada _____	48
6.3.7	Método de desactivación de la clave privada _____	48
6.3.8	Método de destrucción de la clave privada _____	48
<b>6.4.</b>	<b>Otros aspectos de la gestión del par de claves</b> _____	<b>48</b>
6.4.1	Archivo de la clave pública _____	48
6.4.2	Periodo de uso para las claves públicas y privadas _____	48
<b>6.5.</b>	<b>Datos de activación</b> _____	<b>49</b>
6.5.1	Generación y activación de los datos de activación _____	49
6.5.2	Protección de los datos de activación _____	49
6.5.3	Otros aspectos de los datos de activación _____	49
<b>6.6.</b>	<b>Ciclo de vida del dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) y del dispositivo seguro de creación de firma (DSCF)</b> _____	<b>49</b>
<b>6.7.</b>	<b>Controles de seguridad informática</b> _____	<b>50</b>
6.7.1	Requerimientos técnicos de seguridad informática específicos _____	50
6.7.2	Valoración de la seguridad informática _____	50
<b>6.8.</b>	<b>Controles de seguridad del ciclo de vida</b> _____	<b>51</b>
6.8.1	Controles de desarrollo del sistema _____	51
6.8.2	Controles de gestión de la seguridad _____	51



6.8.2.1	Gestión de seguridad _____	51
6.8.2.2	Clasificación y gestión de información y bienes _____	51
6.8.2.3	Operaciones de gestión _____	51
6.8.2.4	Gestión del sistema de acceso _____	52
6.8.2.5	Gestión del ciclo de vida del hardware criptográfico _____	53
6.8.3	Evaluación de la seguridad del ciclo de vida _____	53
<b>6.9.</b>	<b>Controles de seguridad de la red _____</b>	<b>53</b>
<b>6.10.</b>	<b>Controles de ingeniería de los módulos criptográficos _____</b>	<b>54</b>
<b>7.</b>	<b><i>Perfiles de Certificado y CRL</i> _____</b>	<b>55</b>
<b>7.1.</b>	<b>Perfil de Certificado _____</b>	<b>55</b>
7.1.1	Número de versión _____	55
7.1.2	Extensiones del certificado _____	55
7.1.3	Extensión con las facultades de representación especial. _____	55
7.1.4	Extensiones específicas _____	55
7.1.5	Identificadores de objeto (OID) de los algoritmos _____	56
7.1.6	Formato de nombres _____	56
7.1.7	Restricciones de los nombres _____	56
<b>7.2.</b>	<b>Perfil de CRL y extensiones _____</b>	<b>56</b>
<b>7.3.</b>	<b>OCSP Profile _____</b>	<b>56</b>
7.3.1	Número de versión _____	56
7.3.2	Extensiones OCSP _____	56
<b>8.</b>	<b><i>Especificación de la Administración</i> _____</b>	<b>57</b>
<b>8.1.</b>	<b>Autoridad de las políticas _____</b>	<b>57</b>
<b>8.2.</b>	<b>Procedimientos de especificación de cambios _____</b>	<b>57</b>
<b>8.3.</b>	<b>Publicación y copia de la política _____</b>	<b>57</b>
<b>8.4.</b>	<b>Procedimientos de aprobación de la CPS _____</b>	<b>57</b>
	<b><i>Anexo I. Acrónimos</i> _____</b>	<b>58</b>
	<b><i>Anexo II. Definiciones</i> _____</b>	<b>60</b>

# 1. Introducción

## 1.1. Consideración Inicial

Por no haber una definición taxativa de los conceptos de Declaración de Prácticas de Certificación y Políticas de Certificación y debido a algunas confusiones formadas, Camerfirma entiende que es necesario informar de su posición frente a estos conceptos.

**Política de Certificación** es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

**La Declaración de Prácticas de Certificación** es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Suscriptor/creador del sello o Parte usuaria y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aun así es muy importante su interrelación.

Una CPS detallada no forma una base aceptable para la interoperabilidad de Autoridades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes.

En definitiva, una política define “**qué**” requerimientos de seguridad son necesarios para la emisión de los certificados. La CPS nos dice “**cómo**” se cumplen los requerimientos de seguridad impuestos por la política.

## 1.2. Vista General

El presente documento especifica la Política de Certificación para Sello Electrónico de Empresa, y está basada en la especificación del estándar RCF 3647 – *rfc3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, de IETF.

Esta política se encuentra en conformidad con lo dispuesto por la PC de Chambers of Commerce Root, que podrá localizar en la siguiente dirección <http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/> y que establece las normas, políticas y procedimientos para la emisión de certificados de segundo nivel.

Esta política define las reglas y responsabilidades que debe seguir la Autoridad de Certificación de segundo nivel para la emisión de certificados de-sello electrónico, imponiendo además ciertas obligaciones que deben ser tenidas en cuenta por los Suscriptor/creador del sello y Parte usuaria en virtud de su especial relación con este tipo de certificados.

**El certificado de Sello Electrónico es necesario para garantizar el origen, la autenticidad y la integridad de los datos enviados o almacenados electrónicamente y el establecimiento de canales de comunicación seguros. Está pensado para que sea usado por una aplicación ejecutándose en una máquina en procesos de firma automáticos y desasistidos.**

- ✓ Los certificados emitidos bajo esta política requerirán la autenticación de la identidad de los Suscriptor/creadora del sello. Esta identificación y autenticación se realizará según los términos de esta política
- ✓ La AC revocará sus certificados según lo dispuesto en esta política.
- ✓ La AC deberá conservar los registros e incidencias de acuerdo con lo que se establece en esta política.
- ✓ Las funciones críticas del servicio deberán ser realizadas al menos por dos personas.
- ✓ Los certificados de los Suscriptores tienen un periodo de validez determinado por esta política.
- ✓ La información personal recabada del suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación, el cual podrá ejercitar en todo caso sus oportunos derechos de información, rectificación y cancelación. La AC deberá respetar así mismo la normativa aplicable en materia de protección de datos.
- ✓ La actividad de la AC podrá ser sometida a la inspección de la Autoridad de la Políticas (PA) o por personal delegado por la misma.
- ✓ En lo que se refiere al contenido de esta Política de Certificación, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto. En la página Web de Camerfirma ([www.camerfirma.com](http://www.camerfirma.com)) hay algunas informaciones útiles.

### 1.3. Identificación

Certificado	OID Política
Certificado Cualificado de Sello Electrónico en QSCD	[Camerfirma] 1.3.6.1.4.1.17326.10.16.2.1.1  [ETSI EN 319 411 2 - QCP-l-qscd] 0.4.0.194112.1.3
Certificado Cualificado de Sello Electrónico	[Camerfirma] 1.3.6.1.4.1.17326.10.16.2.1.2  [ETSI EN 319 411 2 - QCP-l] 0.4.0.194112.1.1
Certificado de Sello Electrónico	[Camerfirma] 1.3.6.1.4.1.17326.10.16.2.3.2  [ETSI EN 319 411 1 - LCP] 0.4.0.2042.1.3

### 1.4. Comunidad y Ámbito de Aplicación

	SUScriptor/ CREADOR DEL SELLO	SOLICITANTE
<b>Certificado Sello electrónico</b>	Entidad titular de la denominación de sistema o aplicación de proceso automático al que se encuentra asociado el Certificado Digital	Persona física autorizada por la Entidad. En este certificado el Solicitante es el responsable del certificado.

#### **1.4.1 Autoridad de Certificación (AC)**

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor/creador del sello y la Parte usuaria, en las relaciones electrónicas, vinculando una determinada clave pública con una entidad (Suscriptor), a través de la emisión de un Certificado.

#### **1.4.2 Autoridad de Registro (AR)**

En este tipo de certificados la Autoridad de Registro será una Cámara de Comercio o una entidad delegada a tal efecto.

#### **1.4.3 Suscriptor / creador del sello**

Bajo esta Política, el Firmante o creador del sello es una Entidad (empresa u organización de cualquier tipo), titular de la denominación de sistema o aplicación de proceso automático al que se encuentra asociado el Certificado Camerfirma de Sello Electrónico. Por tanto, el creador del sello electrónico es el responsable último de los actos realizados con el certificado.

#### **1.4.4 Parte usuaria**

En esta Política se entiende por Parte usuaria la persona que voluntariamente confía en el Certificado Sello Electrónico de Camerfirma y se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

#### **1.4.5 Solicitante**

A los efectos de esta Política, se entenderá por Solicitante a la persona física autorizada por la Entidad, y que solicita el Certificado Camerfirma de Sello Electrónico. El Solicitante será el responsable de la custodia de las claves y del uso del Certificado.

## 1.4.6 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política, permite identificar a una máquina y su vinculada a una Entidad jurídica titular de la denominación de sistema o aplicación de proceso automático al que se encuentra asociado el Certificado Camerfirma de Sello Electrónico.

### 1.4.6.1 Usos Prohibidos y no Autorizados

Bajo la presente Política no se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Practicas de Certificación.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la AC.

La AC no se responsabilizará **EN NINGÚN CASO** del contenido de la información firmada.

## 1.5. Contacto

La Política de Certificación Camerfirma de Sello Electrónico, está administrada y gestionada por el Departamento Jurídico de Camerfirma SA, pudiendo ser contactado por los siguientes medios:

---

**E-mail:** [juridico@camerfirma.com](mailto:juridico@camerfirma.com)

---

**Dirección:** Camerfirma – Departamento Jurídico  
C/ Ribera del Loira, 12 - 28042 Madrid

---

**Localización:** <https://www.camerfirma.com/address>

---

## **2. Cláusulas Generales**

### **2.1. Obligaciones**

#### **2.1.1 AC**

Las AC's que actúan bajo esta Política de Certificación estarán obligadas a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas de forma segura.
3. Emitir certificados conforme a esta Política y a los estándares de aplicación.
4. Emitir certificados según la información que obra en su poder.
5. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
6. Revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
7. Informar a los Suscriptores de la revocación de sus certificados, en tiempo y forma de acuerdo con la legislación española vigente.
8. Publicar esta Política y las Prácticas correspondientes en su página web
9. Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los Suscriptores.
10. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
11. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

#### **2.1.2 AR**

Las AR's que actúen bajo esta Política de Certificación estarán obligadas a cumplir con lo dispuesto por la normativa vigente y además a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas.

3. Comprobar la identidad de los Solicitantes de Certificados (para el caso de Certificado de Sello Electrónico Cualificado).
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante acerca del Suscriptor.
5. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Solicitante acerca del Suscriptor.
6. Respetar lo dispuesto en los contratos firmados con la AC y con el Solicitante en representación del Firmante.
7. Informar a la AC de las causas de revocación, siempre y cuando tomen conocimiento.

### **2.1.3 Suscriptor /creador del sello**

El Suscriptor de un Certificado Camerfirma de Sello Electrónico, estará obligado a cumplir con lo dispuesto por la normativa aplicable en cada momento y, además, a:

1. Suministrar a la AC la información necesaria para realizar una correcta identificación.
2. Realizar el pago del certificado conforme a la forma y medios establecidos por la AC.
3. Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
4. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

### **2.1.4 Solicitante**

El Solicitante de un certificado Camerfirma estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

1. Suministrar a la AC la información necesaria para realizar una correcta identificación.
2. Custodiar su clave privada de manera diligente
3. Usar el certificado según lo establecido en la presente Política de Certificación
4. Informar de la existencia de alguna causa de revocación.
5. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.



6. En el caso de tratarse de un certificado cualificado deberá identificarse ante la AR.

### **2.1.5 Parte usuaria**

Será obligación de las Partes usuarias cumplir con lo dispuesto por la normativa vigente y, además:

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
2. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

### **2.1.6 Repositorio.**

La información relativa a la publicación y revocación de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente.

La AC deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

## **2.2. Responsabilidad**

La AC dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente.

La AC actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los Solicitantes de los certificados, de los signatarios y de las Partes usuarias que confíen en los certificados.

Las responsabilidades de la AC incluyen las establecidas por la presente Política de Certificación, así como las que resulten de aplicación como consecuencia de la normativa española e internacional.

La AC será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. La exactitud de toda la información contenida en el certificado en la fecha de su emisión
2. La garantía de que la clave pública y privada funcionan conjunta y complementariamente

3. La correspondencia entre el certificado solicitado y el certificado entregado
4. Cualquier responsabilidad que se establezca por la legislación vigente.

### **2.2.1 Exoneración de responsabilidad**

La AC y las AR no serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación
3. Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la AC.
4. Por el uso de la información contenida en el Certificado o en la CRL.
5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Parte usuaria en la normativa vigente, la presente Política de Certificación o en las Prácticas Correspondientes.
6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.
7. Fraude en la información presentada por el solicitante

### **2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones**

La AC y las AR no se responsabilizarán por las pérdidas por transacciones.

## ***2.3. Responsabilidad financiera***

La AC no asume ningún tipo de responsabilidad financiera.

Podrán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

## ***2.4. Interpretación y ejecución***

### **2.4.1 Legislación**

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación española y comunitaria vigentes en cada momento.

## **2.4.2 Independencia**

La invalidez de una de las cláusulas contenidas en esta Política de Certificación no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

## **2.4.3 Notificación**

Cualquier notificación referente a la presente Política de Certificación se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

## **2.4.4 Procedimiento de resolución de disputas**

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte

## **2.5. Tarifas**

### **2.5.1 Tarifas de emisión de certificados y renovación**

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para las Partes usuarias en la página web de Camerfirma.

### **2.5.2 Tarifas de acceso a los certificados**

El acceso a los certificados emitidos es gratuito, no obstante, la AC se reserva el derecho de imponer alguna tarifa para los casos de descarga masiva de CRLs o cualquier otra circunstancia que a juicio de la AC deba ser gravada.

### **2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados**

La AC proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito.

### **2.5.4 Tarifas por el acceso al contenido de estas Políticas de Certificación**

El acceso al contenido de la presente Política de Certificación será gratuito.

## **2.5.5 Política de reintegros**

La AC dispondrá de una política de reintegros puesta a disposición de los usuarios en una dirección de Internet.

## **2.6. *Publicación y repositorios***

### **2.6.1 Publicación de información de la AC**

#### **2.6.1.1 Políticas y Prácticas de Certificación**

La AC estará obligada a publicar la información relativa a sus Políticas y Prácticas de Certificación.

La presente Política de Certificación es pública y se encontrará disponible en Internet.

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en una dirección de Internet.

#### **2.6.1.2 Términos y condiciones**

La AC pondrá a disposición de los Suscriptores y Partes usuarias los términos y condiciones del servicio. En concreto:

- a) La AC pondrá a disposición de los Suscriptores y Partes usuarias los términos y condiciones relativos al uso de los certificados;

Las limitaciones de uso.

La información sobre cómo validar los certificados, incluyendo los requisitos para comprobar si un certificado ha sido revocado.

Los límites de responsabilidad.

El periodo de tiempo en que la información registrada será almacenada.

Los procedimientos para la resolución de disputas.

El ordenamiento jurídico aplicable.

Si la AC ha sido acreditada conforme a la Política identificada en el certificado.

- b) La información referida en el apartado anterior estará disponible a través de un medio de comunicación duradero, podrá ser transmitida electrónicamente y estará escrita en un lenguaje fácilmente comprensible.

### **2.6.1.3 Difusión de los certificados**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para los Suscriptores y Partes usuarias.

En concreto:

- a) El certificado de la AC es público y se encontrará disponible en la página web de Camerfirma.
- b) La AC tendrá un mecanismo de distribución a los usuarios de los certificados emitidos sólo en los casos en que el Suscriptor haya otorgado su consentimiento
- c) La AC pondrá a disposición de las Partes usuarias los términos y condiciones referentes al uso de los certificados
- d) La información a la que se refiere el punto a) estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la AC, la AC hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

### **2.6.2 Frecuencia de publicación**

Las Políticas y Prácticas de Certificación se publicarán una vez hayan sido creadas o en el momento en que se apruebe una modificación de las mismas.

La CRL que contiene la lista de los certificados revocados se publicará con una frecuencia mínima diaria.

### **2.6.3 Controles de acceso**

El acceso a la información será gratuito y estará a disposición de los Suscriptores y Partes usuarias.

La AC podrá establecer sistemas de seguridad para controlar el acceso a la información contenida en el web, LDAP o CRL con el fin de evitar usos indebidos que afecten la protección de datos personales.

## **2.7. Auditorias**

### **2.7.1 Frecuencia de las auditorias**

Se realizará una auditoria con una periodicidad mínima anual, salvo que se establezca un plazo menor por la normativa vigente.

## **2.7.2 Identificación y calificación del auditor**

El auditor debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos.

## **2.7.3 Relación entre el auditor y la AC**

La auditoría deberá ser realizada por un auditor independiente y neutral.

No obstante, lo anterior no impedirá la realización de auditorías internas periódicas.

## **2.7.4 Tópicos cubiertos por la auditoría**

La auditoría deberá verificar en todo caso:

- a) Que la AC tiene un sistema que garantice la calidad del servicio prestado
- b) Que la AC cumple con los requerimientos de esta Política de Certificación
- c) Que las Prácticas de Certificación de la AC se ajustan a lo establecido en esta Política, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.

## **2.8. Confidencialidad**

### **2.8.1 Tipo de información a mantener confidencial**

Se determinará por la AC la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la normativa vigente en materia de protección de datos y concretamente con lo dispuesto por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

### **2.8.2 Tipo de información considerada no confidencial**

Se considerará como información no confidencial:

- a) La contenida en la presente Política y en las Prácticas de Certificación
- b) La información contenida en los certificados siempre que el Suscriptor haya otorgado su consentimiento
- c) Cualquier información cuya publicidad sea impuesta normativamente

- d) Las que así se determinen por las Prácticas de Certificación siempre que no contravengan ni la normativa vigente ni lo dispuesto en esta Política de Certificación.

### **2.8.3 Divulgación de información de revocación de certificados**

La forma de difundir la información relativa a la revocación de un certificado se realizará mediante la publicación de las correspondientes CRLs.

### **2.8.4 Envío a la Autoridad Competente**

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

## ***2.9. Derechos de propiedad intelectual***

La AC es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificación. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la AC sin la autorización expresa por su parte. No obstante, no necesitará autorización de la AC para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta Política de Certificación.

## **3. Identificación y Autenticación**

### ***3.1. Registro inicial***

#### **3.1.1 Tipos de nombres**

Todos los Suscriptores requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

#### **3.1.2 Pseudónimos**

No estipulado.

#### **3.1.3 Reglas utilizadas para interpretar varios formatos de nombres**

Se atenderá en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

#### **3.1.4 Unicidad de los nombres**

La AC se asegurará de que no existan dos certificados activos emitidos con igual titular teniendo estos titulares diferentes identidades.

#### **3.1.5 Procedimiento de resolución de disputas de nombres**

Se atenderá a lo dispuesto en el apartado 2.4.4 de este documento

#### **3.1.6 Reconocimiento, autenticación y función de las marcas registradas**

Se podrá admitir la identificación en función de marcas registradas. La AC no asumirá ninguna responsabilidad respecto del uso de marcas u otros signos distintivos, registrados o no, en la emisión de los Certificados expedidos bajo la presente Política de Certificación.

#### **3.1.7 Métodos de prueba de la posesión de la clave privada**

El prestador deberá definir un procedimiento que garantice la posesión de la clave privada por parte del suscriptor si éste genera el par de claves.

Si es el prestador quien genera el par de claves deberá definir un procedimiento seguro de entrega de las claves al suscriptor.



### **3.1.8 Autenticación de la identidad de una Entidad**

La AC deberá asegurarse la existencia de la Entidad que aparece en el certificado digital, estableciendo los procesos adecuados para realizar esta comprobación bien con medios propios o con la consulta a registros externos.

### **3.1.9 Autorización de la Entidad al Solicitante**

Para solicitar los certificados emitidos bajo esta Política, el Solicitante deberá acreditar su identidad conforme dispone la legislación vigente y que está debidamente autorizado por el Suscriptor (la Entidad) para solicitar el certificado de sello electrónico.

Para la comprobación de la identidad del Solicitante se exigirá su presencia física y la entrega de la copia y del original (para su cotejo) de su documento de identidad.

Para comprobar que el Solicitante está autorizado por el Suscriptor para solicitar el certificado de sello electrónico, se exigirá la entrega de una autorización específica firmada por alguien con poder de representación suficiente de la Entidad creadora del sello, acompañada con una copia del documento de identidad del autorizante.

## ***3.2. Renovación de la clave***

La AC deberá informar al Suscriptor antes de renovar de los términos y condiciones que hayan cambiado respecto de la anterior emisión.

La AC en ningún caso emitirá un nuevo certificado conteniendo la anterior clave pública del Suscriptor.

Un certificado podrá ser renovado por un periodo máximo de 5 años, debiendo proceder a una nueva solicitud una vez transcurrido este plazo siguiendo el procedimiento empleado para una primera solicitud.

La personación física del Solicitante puede no ser necesaria cuando la solicitud de renovación se realice de forma on-line por medio del certificado que se pretende renovar. No obstante lo anterior, se exigirá personación física siempre que hayan transcurrido más de 5 años desde la última verificación de la identidad realizada mediante la personación física del solicitante.

## ***3.3. Modificación de certificados***

Ante cualquier necesidad de modificación de certificados, la AC realizará una revocación del certificado y una nueva emisión con los datos corregidos, tal y como se indica en el apartado 3.6 de la DPC.

### ***3.4. Reemisión después de una revocación***

La AC no realizará reemisiones

### ***3.5. Solicitud de revocación***

Todas las solicitudes de revocación deberán ser autenticadas tal y como se indica en el apartado 4.5 de la Declaración de Prácticas de Certificación.

## **4. Requerimientos Operacionales**

### ***4.1. Solicitud de certificados***

#### **Registro**

Antes de comenzar el procedimiento de emisión, la AC deberá informar al Suscriptor de los términos y condiciones relativos al uso del certificado. La AC deberá comunicar esta información a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

El Solicitante deberá facilitar su dirección física u otros datos que permitan contactar con él.

La AC deberá cumplir con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos.

### ***4.2. Petición de certificación cruzada***

La AC identificará los procesos necesarios para realizar certificación cruzada.

La AC deberá revisar cualquier petición de certificación cruzada y aprobar o denegar dicha petición.

Una petición de certificación cruzada deberá incluir en todo caso su política de certificación, un informe de auditoría externa aprobando el nivel de seguridad establecido en la política de certificación y la clave pública de verificación de la AC.

### ***4.3. Emisión de certificados***

La AC deberá poner todos los medios a su alcance para asegurar que la emisión y renovación de certificados se realiza de una forma segura. En particular:

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los DN asignados a los Suscriptores.

La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Suscriptor o entre distintos componentes del sistema de certificación.

La AC deberá verificar que el registro de los datos es intercambiado con proveedores de servicios reconocidos, cuya identidad es autenticada.

La AC Comprobara la existencia del solicitante y de la organización representada en el certificado, verificará los datos entregados por el solicitante bien sea por medios propios o de terceros.

La AC deberá notificar al solicitante la emisión de su certificado.

#### ***4.4. Aceptación de certificados***

A partir de la entrega del certificado, el Suscriptor dispondrá de un periodo de catorce días naturales para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a la AC y el contenido del certificado, ello deberá ser comunicado de inmediato a la AC para que proceda a su revocación y a la emisión de un nuevo certificado. La AC entregará el nuevo certificado sin coste para el Suscriptor en el caso de que la diferencia entre los datos sea causada por un error no imputable al Suscriptor. Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el Suscriptor ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, el Suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

#### ***4.5. Suspensión y revocación de certificados***

##### **4.5.1 Causas de revocación**

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

Solicitud voluntaria del Suscriptor.

Fallecimiento del Suscriptor (si es persona física) o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación o extinción de la entidad.

Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

Inexactitudes graves en los datos aportados por el Solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.

Que se detecte que las claves privadas del Suscriptor o de la AC han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por

cualesquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.

Por incumplimiento por parte de la AC, del Solicitante o del Suscriptor de las obligaciones establecidas en esta política.

Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.

Por resolución judicial o administrativa que lo ordene.

Por la concurrencia de cualquier otra causa especificada en la presente política.

#### **4.5.2 Quién puede solicitar la revocación**

La revocación de un certificado podrá solicitarse únicamente por el representante o poderdante de la Entidad (quien otorga al Solicitante la autorización en nombre y representación de la entidad), por el propio Suscriptor o por la propia AC.

Todas las solicitudes deberán ser en todo caso autenticadas.

#### **4.5.3 Procedimiento de solicitud de revocación**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son revocados basándose en peticiones de revocación autorizadas y validadas.

La información relativa al retraso máximo entre la recepción de una petición de revocación y su paso al estado de suspendido estará disponible para todas las Partes usuarias. Este deberá ser como máximo de 3 horas

El Suscriptor cuyo certificado haya sido revocado deberá ser informado del cambio de estado de su certificado. La AC utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

Una vez que un certificado es revocado, este no podrá volver a su estado activo. La revocación de un certificado es una acción, por tanto, definitiva.

La CRL, en su caso, será firmada por la AC o por una autoridad de confianza de la AC.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la AC, la AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la autenticidad y la confidencialidad de la información relativa al estado de los certificados.

La información relativa al estado de los certificados deberá estar disponible públicamente.

#### **4.5.4 Periodo de revocación**

La decisión de revocar o no un certificado no podrán retrasarse por un periodo máximo de 2 semanas.

#### **4.5.5 Suspensión**

La suspensión, a diferencia de la revocación supone la pérdida de validez temporal de un certificado.

#### **4.5.6 Procedimiento para la solicitud de suspensión**

La solicitud de suspensión se realizará a través de una llamada telefónica al servicio de gestión de las revocaciones o por medio de un servicio on-line de suspensiones en la página web de la AC.

#### **4.5.7 Límites del periodo de suspensión**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que un certificado no permanece suspendido por más tiempo que el necesario para confirmar la procedencia o no de la revocación.

#### **4.5.8 Frecuencia de emisión de CRL's**

La AC proporcionará la información relativa a la revocación de los certificados a través de una CRL.

La AC actualizará y publicará la CRL dentro de las 3 horas siguientes a la recepción de una solicitud de suspensión que haya sido previamente validada, y al menos con una frecuencia semanal si no se han producido cambios en la CRL.

#### **4.5.9 Requisitos de comprobación de CRL's**

Las Partes usuarias podrán comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida. No obstante, la AC podrá imponer una tarifa por el acceso a la CRL.

#### **4.5.10 Disponibilidad de comprobación on-line de la revocación**

Se proporcionará un servicio on-line de comprobación de revocaciones, el cual estará disponible las 24 horas del día los 7 días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de la AC, la AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

#### **4.5.11 Requisitos de la comprobación on-line de la revocación**

La Parte usuaria que desee comprobar la revocación de un certificado, podrá hacerlo de forma on-line a través de la página web de la AC [www.camerfirma.com](http://www.camerfirma.com).

La AC dispondrá de un sistema de consulta que impida la obtención masiva de datos relativos a los Suscriptores, por lo que para la obtención del estado de un certificado deberán conocerse algunos parámetros del mismo como el e-mail.

No obstante lo anterior, el acceso a este sistema de consulta de certificados será libre y gratuito.

#### **4.5.12 Otras formas de divulgación de información de revocación disponibles**

No estipulado.

#### **4.5.13 Requisitos de comprobación para otras formas de divulgación de información de revocación**

No estipulado

#### **4.5.14 Requisitos especiales de revocación por compromiso de las claves**

No estipulado

## **4.6. Procedimientos de Control de Seguridad**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a un certificado es conservada durante el periodo de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales. En particular:

### **General**

- a) Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la confidencialidad y la integridad de los registros relativos a los certificados, tanto de los actuales como de aquellos que hayan sido previamente almacenados.
- b) Los registros relativos a los certificados deberán ser almacenados completa y confidencialmente de acuerdo con las prácticas de negocio.
- c) Los registros relativos a los certificados deberán estar disponibles si estos son requeridos a efectos probatorios en los procedimientos legales.
- d) El momento exacto en que se produjeron los eventos relativos a la gestión de los certificados deberá ser almacenado.
- e) Los registros relativos a los certificados serán mantenidos durante un periodo de tiempo necesario para dotar de la evidencia legal necesaria a las firmas electrónicas.
- f) Los eventos se registrarán de manera que no puedan ser fácilmente borrados o destruidos (excepto para su transferencia a medios duraderos) durante el periodo de tiempo en el que deban ser conservados
- g) Los eventos específicos y la fecha de registro serán documentados por la AC

### **Registro**

- h) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que todos los eventos relativos al registro, incluyendo las peticiones de renovación y revocación serán registrados.
- i) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada
- j) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la privacidad de la información relativa al suscriptor.

### **Generación del certificado**

- k) La AC registrará todos los eventos relativos al ciclo de vida de las claves de la AC
- l) La AC registrará todos los eventos relativos al ciclo de vida de los certificados

### **Gestión de la revocación**

- m) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las peticiones e informes relativos a una revocación, así como su resultado, son registrados.



#### **4.6.1 Tipos de eventos registrados**

Toda la información auditada y especificada en el apartado anterior deberá ser archivada.

La AC registrará y guardará los logs de todos los eventos relativos al sistema de seguridad de la AC. Estos incluirán eventos como:

- encendido y apagado del sistema
- encendido y apagado de la aplicación de la AC
- intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- cambios en los detalles de la AC y/o sus claves
- cambios en la creación de políticas de certificados
- intentos de inicio y fin de sesión
- intentos de accesos no autorizados al sistema de la AC a través de la red.
- intentos de accesos no autorizados al sistema de archivos
- generación de claves propias
- creación y revocación de certificados
- intentos de dar de alta, eliminar, habilitar y deshabilitar Suscriptores y actualizar
- acceso físico a los logs
- cambios en la configuración y mantenimiento del sistema
- cambios personales

#### **4.6.2 Frecuencia de procesado de Logs**

La CA deberá revisar sus logs periódicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente.

La CA deberá así mismo asegurarse de que los logs no han sido manipulados y deberán documentar las acciones tomadas ante esta revisión

#### **4.6.3 Periodos de retención para los Logs de auditoría**

La información almacenada deberá ser conservada al menos durante 5 años.

#### **4.6.4 Protección de los Logs de auditoría**

El soporte de almacenamiento de los logs debe ser protegido por seguridad física, o por una combinación de seguridad física y protección criptográfica. Además, será adecuadamente protegido de amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

#### **4.6.5 Procedimientos de backup de los Logs de auditoría**

Debe establecerse un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

#### **4.6.6 Sistema de recogida de información de auditoría**

No estipulado.

#### **4.6.7 Notificación al sujeto causa del evento**

No estipulado.

#### **4.6.8 Análisis de vulnerabilidades**

Se deberá realizar una revisión de riesgos de seguridad para la totalidad del sistema. Esta revisión cubrirá la totalidad de riesgos que pueden afectar a la emisión de certificados y se realizará con una periodicidad anual.

### ***4.7. Archivo de registros***

#### **4.7.1 Tipo de archivos registrados**

Los siguientes datos y archivos deben ser almacenados por la AC o por delegación de esta.

todos los datos relativos a los certificados.

solicitudes de emisión y revocación de certificados

todos los certificados emitidos o publicados

CRLs emitidas o registros del estado de los certificados generados

La AC es responsable del correcto archivo de todo este material

#### **4.7.2 Periodo de retención para el archivo**

Los certificados se conservarán durante al menos un año desde su expiración. La información relativa a la identificación y autenticación del Suscriptor deberá ser conservada durante al menos 15 años.

#### **4.7.3 Protección del archivo**

El soporte de almacenamiento debe ser protegido por medio de seguridad física, o por una combinación de seguridad física y protección criptográfica. Además, el soporte será adecuadamente protegido amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

#### **4.7.4 Procedimientos de backup del archivo**

Debe establecerse un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes estén disponibles en un periodo corto de tiempo las correspondientes copias de backup.

#### **4.7.5 Requerimientos para el sellado de tiempo de los registros**

No estipulado

#### **4.7.6 Sistema de recogida de información de auditoria**

No estipulado

#### **4.7.7 Procedimientos para obtener y verificar información archivada**

La AC dispondrá de un procedimiento adecuado que limite la obtención de información sólo a las personas debidamente autorizadas.

Este procedimiento deberá regular tanto los accesos a la información internos como externos, debiendo exigir en todo caso un acuerdo de confidencialidad previo a la obtención de la información.

### ***4.8. Cambio de clave de la AC***

Antes de que el uso de la clave privada de la CA caduque se deberá realizar un cambio de claves. La vieja CA y su clave privada se desactivarán y se generará una nueva CA con una clave privada nueva y un nuevo DN.

## ***4.9. Recuperación en caso de compromiso de la clave o desastre***

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar en caso de desastre o compromiso de la clave privada de la AC que éstas serán restablecidas tan pronto como sea posible. En particular:

### **4.9.1 La clave de la AC se compromete**

El plan de la continuidad de negocio de la AC (o el plan de contingencia) tratará el compromiso o el compromiso sospechado de la clave privada de la AC como un desastre.

En caso de compromiso, la AC tomará como mínimo las siguientes medidas:

Informar a todos los Suscriptores, Partes usuarias y otras ACs con los cuales tenga acuerdos u otro tipo de relación del compromiso.

Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.

### **4.9.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre**

La AC debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

La AC debe reestablecer los servicios de acuerdo con esta política dentro de las 24 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal restablecimiento.

## ***4.10. Cese de la AC***

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los Suscriptores o Partes usuarias como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular:

a) Antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:

Informar a todos los Suscriptores, Partes usuarias y otras ACs con los cuales tenga acuerdos u otro tipo de relación del cese.

La AC revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.

La AC realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los Suscriptores y Partes usuarias.

Las claves privadas de la AC serán destruidas o deshabilitadas para su uso.

b) La AC tendrá contratado un seguro que cubra hasta el límite contratado los costes necesarios para satisfacer estos requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.

c) Se establecerán en la DPC/CPS las previsiones hechas para el caso de cese de actividad. Estas incluirán:

informar a las entidades afectadas

transferencia de las obligaciones de la AC a otras partes

cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aún no ha expirado.

En particular, la AC deberá:

Informar puntualmente a todos los Suscriptores, empleados y Partes usuarias con una anticipación mínima de 6 meses antes del cese

Transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación

## **5. Controles de Seguridad Física, Procedimental y de Personal**

### ***5.1. Controles de Seguridad física***

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados. En particular:

#### **AC General**

El acceso físico a las instalaciones vinculadas a la generación de certificados y servicios de gestión de revocaciones deberá ser limitado a las personas autorizadas y las instalaciones en las que se firman los certificados deberán ser protegidas de las amenazas físicas.

Se establecerán controles para impedir la pérdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad

Se establecerán controles para evitar el compromiso o robo de información

#### **Emisión de certificados y gestión de revocaciones.**

Las actividades relativas a la emisión de certificados y gestión de revocaciones serán realizadas en un espacio protegido físicamente de accesos no autorizados al sistema o a los datos.

La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la emisión de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro.

Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en si mismos y las instalaciones usadas para soportar sus operaciones. Los programas de seguridad física y medioambiental de la AC relativos a la generación de certificados y servicios de gestión de revocaciones estarán provistos de controles de acceso físico, protección ante desastres naturales, sistemas anti-incendios, fallos eléctricos y de telecomunicaciones, humedad, protección antirrobo, ...

Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de la AC sean sacados de las instalaciones sin autorización.

### **5.1.1 Ubicación y construcción**

Las instalaciones de la AC deben estar ubicadas en una zona de bajo riesgo de desastres y que permita un rápido acceso a las mismas conforme al plan de contingencias.

Así mismo, las instalaciones estarán equipadas con los elementos y materiales adecuados para poder albergar información de alto valor.

### **5.1.2 Acceso físico**

El acceso físico a las zonas de seguridad estará limitado al personal autorizado previa autenticación.

### **5.1.3 Alimentación eléctrica y aire acondicionado**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la alimentación eléctrica y el aire acondicionado son suficientes para soportar las actividades del sistema de la AC.

### **5.1.4 Exposición al agua**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de AC está protegido de la exposición al agua.

### **5.1.5 Protección y prevención de incendios**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de AC está protegido con un sistema anti-incendios.

### **5.1.6 Sistema de almacenamiento.**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de almacenamiento usado por el sistema de AC está protegido de riesgos medioambientales como la temperatura, el fuego, la humedad y la magnetización.

### **5.1.7 Eliminación de residuos**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos de la AC serán destruidos, así como que la información que contengan será irrecuperable.

### 5.1.8 Backup remoto

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las instalaciones usadas para realizar back-up externo, que tendrán el mismo nivel de seguridad que las instalaciones principales.

## 5.2. *Controles procedimentales.*

### 5.2.1 Roles de confianza

Los roles de confianza, en los cuales se sustenta la seguridad de la AC, serán claramente identificados.

Los roles de confianza incluyen las siguientes responsabilidades:

**Responsable de seguridad:** asume la responsabilidad por la implementación de las políticas de seguridad, así como gestión y revisión de logs.

**Administradores de sistema:** Están autorizados para instalar, configurar y mantener de los sistemas y aplicaciones de confianza de la AC que soportan las operaciones de Certificación.

**Operador de sistema:** Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación.

**Administrador de CA:** Responsable de la Administración y control de gestión de los sistemas de confianza de la AC.

**Operador de CA:** Realizan funciones de apoyo en el control dual de las operaciones de la CA.

**Auditor de CA:** Realiza las labores de supervisión y control de la implementación de las políticas de seguridad.

La AC debe asegurarse que existe una separación de tareas para las funciones críticas de la CA, para prevenir que una persona use el sistema el sistema de AC y la clave de la CA sin detección.

La separación de los roles de confianza será detallada en la CPS.

### 5.2.2 Número de personas requerido por tarea

Las siguientes tareas requerirán al menos un control dual:

La generación de la clave de la AC.

La recuperación y back-up de la clave privada de la AC.



Activación de la clave privada de la AC.

Cualquier actividad realizada sobre los recursos HW y SW que dan soporte a la autoridad de certificación.

### **5.2.3 Identificación y autenticación para cada rol**

La AC establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

## **5.3. Controles de seguridad de personal**

### **5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal cumple con los requisitos mínimos razonables para el desempeño de sus funciones. En concreto:

#### **AC General**

- a) La AC empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.
- b) Los roles de seguridad y responsabilidades especificadas en la política de seguridad de la AC, serán documentadas en la descripción del trabajo.
- c) Se deberá describir el trabajo del personal de la AC (temporal y fijo) desde el punto de vista de realizar una separación de tareas, definiendo los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones específicas de la AC.
- d) El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

#### **Registro, generación de certificados y gestión de revocaciones**

- e) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.
- f) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la AC.
- g) El personal de la AC será formalmente designado para desempeñar roles de confianza por el responsable de seguridad.

- h) La AC no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

### **5.3.2 Procedimientos de comprobación de antecedentes**

La AC no podrá asignar funciones que impliquen el manejo de elementos críticos del sistema a aquellas personas que no posean la experiencia necesaria en la propia AC que propicie la confianza suficiente en el empleado. Se entenderá como experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 6 meses.

### **5.3.3 Requerimientos de formación**

La AC debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de AC o AR, recibirá una formación relativa a:

Los principales mecanismos de seguridad de AC y/o AR.

Todo el software de PKI y sus versiones empleados en el sistema de la AC.

Todas las tareas de PKI que se espera que realicen.

Los procedimientos de resolución de contingencias y continuidad de negocio.

### **5.3.4 Requerimientos y frecuencia de la actualización de la formación**

La formación debe darse con una frecuencia anual para asegurar que el personal está desarrollando sus funciones correctamente.

### **5.3.5 Frecuencia y secuencia de rotación de tareas**

No estipulado.

### **5.3.6 Sanciones por acciones no autorizadas**

La AC deberá fijar las posibles sanciones por la realización de acciones no autorizadas.

### **5.3.7 Requerimientos de contratación de personal**

Ver el apartado 5.3.1 de este documento.

### **5.3.8 Documentación proporcionada al personal**

Todo el personal de la AC deberá recibir los manuales de usuario en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, revocación y la funcionalidad del software empleado.

## **6. Controles de Seguridad Técnica**

### ***6.1. Generación e instalación del par de claves***

#### **6.1.1 Generación del par de claves de la AC**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de la AC sean generadas de acuerdo a los estándares.

En particular:

- a) La generación de la clave de la AC se realizará en un entorno securizado físicamente por el personal adecuado según los roles de confianza y, al menos con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS.
- b) La generación de la clave de la AC se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-2, en su nivel 3 o superior.

#### **6.1.2 Generación del par de claves del Suscriptor**

El par de claves será generado por el emisor o bajo su control

Si las claves del suscriptor son generadas por la AC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves son generadas de forma segura y que se mantendrá la privacidad de las mismas. En particular:

- a) Las claves serán generadas usando un algoritmo adecuado para los propósitos de la firma electrónica avanzada.
- b) Las claves tendrán una longitud de clave adecuada para los propósitos de la firma electrónica avanzada y para el algoritmo de clave pública empleado.
- c) Las claves serán generadas y guardadas de forma segura antes de entregárselas al responsable de la entidad.
- d) Las claves serán destruidas de forma segura después de su entrega al responsable de la entidad.

#### **6.1.3 Entrega de la clave privada al Suscriptor**

Cuando la clave privada del Suscriptor sea generada por la AC, ésta le será entregada de manera que la confidencialidad de la misma no sea comprometida y sólo el Suscriptor tenga acceso a la misma.

La clave privada deberá ser almacenada en todo caso en un dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) o en dispositivo seguro de creación de firma (DSCF).

Así mismo, este dispositivo seguro podrá consistir en un medio de almacenamiento externo (p. ej smartcard o key token) o bien en un medio software (p. ej. PKCS12).

Cuando la AC entrega un dispositivo seguro al responsable de la entidad, deberá hacerlo de forma segura. En particular:

- a) La preparación del dispositivo seguro, deberá ser controlada de manera segura por el proveedor de servicios.
- b) El dispositivo seguro será guardado y distribuido de forma segura.
- c) Cuando el dispositivo seguro tenga asociado unos datos de activación de Tercero que confía (p.ej. un código PIN), los datos de activación se deberán preparar de forma segura y distribuirse de manera separada del dispositivo seguro de creación de firma.

#### **6.1.4 Entrega de la clave pública del Firmante al emisor del certificado**

Cuando el Suscriptor pueda generar sus propias claves, la clave pública del Suscriptor tiene que ser transferida a la AR o AC, de forma que se asegure que,

- no ha sido cambiado durante el traslado.
- el remitente está en posesión de la clave privada que se corresponde con la clave pública transferida y
- el proveedor de la clave pública es la legítima Parte usuaria que aparece en el certificado

#### **6.1.5 Entrega de la clave pública de la CA a los Usuarios**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de la clave pública de la AC y los parámetros a ella asociados son mantenidos durante su distribución a las Partes usuarias. En particular:

- a) La clave pública de la AC estará disponible a las Partes usuarias de manera que se asegure la integridad de la clave y se autentique su origen.
- b) El certificado de la AC y su fingerprint (huella digital) estarán a disposición de las Partes usuarias a través de su página web.

#### **6.1.6 Tamaño y periodo de validez de las claves del emisor**

El emisor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits para firmar certificados.

El periodo de uso de una clave privada será como máximo de 24 años, después del cual deberán cambiarse estas claves.

El periodo de validez del certificado de la AC se establecerá como mínimo en atención a lo siguiente:

- El periodo de uso de la clave privada de la AC, y
- El periodo máximo de validez de los certificados de los Suscriptores firmados con esa clave

### **6.1.7 Tamaño y periodo de validez de las claves del Suscriptor**

El Suscriptor deberá usar claves basadas en el algoritmo RSA con una longitud mínima de **2048** bits.

El periodo de uso de la clave pública y privada del Suscriptor no deberá ser superior a **4 años** y no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

### **6.1.8 Parámetros de generación de la clave pública**

No estipulado.

### **6.1.9 Comprobación de la calidad de los parámetros**

No estipulado.

### **6.1.10 Hardware / software de generación de claves**

El par de claves de los Suscriptores serán generadas por el prestador o CA.

### **6.1.11 Fines del uso de la clave**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves de firma de la CA son usadas sólo para los propósitos de generación de certificados y para la firma de CRLs

## ***6.2. Protección de la clave privada***

### **De la AC**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves privadas de la AC continúan siendo confidenciales y mantienen su integridad. En particular:

- a) La clave privada de firma de la AC será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-2, en su nivel 3 o superior.

- b) Cuando la clave privada de la AC esté fuera del módulo criptográfico esta deberá estar cifrada.
- c) Se deberá hacer un back up de la clave privada de firma de la CA, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS.
- d) Las copias de back up de la clave privada de firma de la CA se registrarán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

### **6.3. Estándares para los módulos criptográficos**

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

#### **6.3.1 Control multi-persona (n de entre m) de la clave privada**

Se requerirá un control multi-persona para la activación de la clave privada de la CA. Este control deberá ser definido adecuadamente por la CPS en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

#### **6.3.2 Depósito de la clave privada (key escrow)**

La clave privada de la AC debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

La clave privada del usuario solo podrá almacenarse por la AC salvo en caso de su gestión en nombre de éste, quien deberá mantener un control exclusivo sobre el uso de tal clave privada.

#### **6.3.3 Copia de seguridad de la clave privada**

La AC deberá realizar una copia de back up de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado anterior.

Las copias de las claves privadas del Suscriptor se registrarán por lo dispuesto en el punto anterior.

#### **6.3.4 Archivo de la clave privada**

La clave privada de la AC no podrá ser archivada de acuerdo una vez finalizado su ciclo de vida.

Las claves privadas del Suscriptor pueden ser archivadas en caso de su gestión en nombre de éste.

### **6.3.5 Introducción de la clave privada en el módulo criptográfico**

Ya visto.

### **6.3.6 Método de activación de la clave privada**

La clave privada de la AC deberá ser activada conforme al apartado 6.3.1.

No aplicable a la clave privada del Suscriptor.

### **6.3.7 Método de desactivación de la clave privada**

La clave de CA se desactivará siguiendo los procesos operativos y técnicos descritos por el fabricante del dispositivo donde esté almacenada y mediante un control dual.

### **6.3.8 Método de destrucción de la clave privada**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la CA no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la CA deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

La destrucción o deshabilitación de las claves se detallará en un documento creado al efecto.

## ***6.4. Otros aspectos de la gestión del par de claves***

### **6.4.1 Archivo de la clave pública**

La AC deberá conservar todas las claves públicas de verificación.

### **6.4.2 Periodo de uso para las claves públicas y privadas**

Ya visto.



## **6.5. Datos de activación**

### **6.5.1 Generación y activación de los datos de activación**

Los datos de activación de las AC se generan y se almacenan en smart cards criptográficas únicamente en posesión de personal autorizado.

### **6.5.2 Protección de los datos de activación**

Solo el personal autorizado conoce los PINs y contraseñas para acceder a los datos de activación.

### **6.5.3 Otros aspectos de los datos de activación**

No estipulados.

## **6.6. Ciclo de vida del dispositivo seguro de almacenamiento de los datos de creación de firma (DSADCF) y del dispositivo seguro de creación de firma (DSCF)**

La AC deberá, por si misma o por delegación de esta función, realizar los mayores para asegurar que:

- a) La preparación del DSADCF o DSCF es controlada de forma segura.
- b) El DSADCF o DSCF es almacenado y distribuido de forma segura.
- c) Si el propio sistema lo permite, que la activación y desactivación del DSADCF o DSCF es controlada de forma segura.
- d) El DSADCF o DSCF no es usado por la CA o entidad delegada antes de su emisión.
- e) El DSADCF o DSCF queda inhabilitado para su uso en caso de ser devuelto por el Suscriptor.
- f) Cuando el DSADCF o DSCF lleve asociado unos datos de activación (p.ej. PIN), estos datos de activación y el dispositivo seguro de creación de firma serán preparados y distribuidos de forma separada.

## **6.7. Controles de seguridad informática**

La AC empleará sistemas fiables y productos que estén protegidos contra modificaciones. En particular, los sistemas deberán cumplir las siguientes funciones:

identificación de todos los usuarios

controles de acceso basados en privilegios

control dual para ciertas operaciones relativas a la seguridad

generación de logs, revisión de auditoría y archivo de todos los eventos relacionados con la seguridad.

back up y recuperación

### **6.7.1 Requerimientos técnicos de seguridad informática específicos**

Cada servidor de AC incluirá las siguientes funcionalidades:

control de acceso a los servicios de AC y gestión de privilegios

imposición de separación de tareas para la gestión de privilegios

identificación y autenticación de roles asociados a identidades

archivo del historial del suscriptor y la AC y datos de auditoría

auditoría de eventos relativos a la seguridad

auto-diagnóstico de seguridad relacionado con los servicios de la AC

Mecanismos de recuperación de claves y del sistema de AC

Las funcionalidades de arriba pueden ser provistas por el sistema operativo o mediante una combinación de sistemas operativos, software de PKI y protección física.

### **6.7.2 Valoración de la seguridad informática**

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

## **6.8. Controles de seguridad del ciclo de vida**

### **6.8.1 Controles de desarrollo del sistema**

La AC empleará sistemas fiables y productos que estén protegidos contra modificaciones. Esta información es confidencial y solo se proporciona a quien acredita la necesidad de conocerlos.

### **6.8.2 Controles de gestión de la seguridad**

#### **6.8.2.1 Gestión de seguridad**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los procedimientos administrativos y de gestión son aplicados, son adecuados y se corresponden con los estándares reconocidos. En particular:

- a) La AC será responsable por todos los aspectos relativos a la prestación de servicios de certificación, incluso si algunas de sus funciones han sido subcontratadas con terceras partes. Las responsabilidades de las terceras partes serán claramente definidas por la AC en los acuerdos concretos que la AC suscriba con esas terceras partes para asegurar que éstas están obligadas a implementar cualquier control requerido por la AC. La AC será responsable por la revelación de prácticas relevantes.
- b) La AC deberá desarrollar las actividades necesarias para la formación y concienciación de los empleados en material de seguridad.
- c) La información necesaria para gestionar la seguridad de la AC deberá mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado previamente.
- d) Los controles de seguridad y procedimientos operativos para las instalaciones de la AC, sistemas e información necesarios para los servicios de certificación serán documentados, implementados y mantenidos.
- e) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se mantendrá la seguridad de información cuando la responsabilidad respecto a funciones de la AC haya sido subcontratada a otra organización

#### **6.8.2.2 Clasificación y gestión de información y bienes**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus activos y su información reciben un nivel de protección adecuado. En particular, la AC mantendrá un inventario de toda la información y hará una clasificación de los mismos y sus requisitos de protección en relación al análisis de sus riesgos.

#### **6.8.2.3 Operaciones de gestión**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los sistemas de la AC son seguros, son tratados correctamente, y con el mínimo riesgo de fallo. En particular:

- a) Se protegerá la integridad de los sistemas de AC y de su información contra virus y software malintencionado o no autorizado
- b) Los daños derivados de incidentes de seguridad y los errores de funcionamiento deberán ser minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.
- c) Los soportes serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados
- d) Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de certificación.

### **Tratamiento de los soportes y seguridad**

- e) Todos los soportes serán tratados de forma segura de acuerdo con los requisitos del plan de clasificación de la información. Los soportes que contengan datos sensibles serán destruidos de manera segura si no van a volver a ser requeridos

### **Planning del sistema**

- f) Se deberá controlar la capacidad de atención a la demanda y la previsión de futuros requisitos de capacidad para asegurar la disponibilidad de recursos y de almacenamiento.

### **Reportes de incidencias y respuesta**

- g) La AC responderá de manera inmediata y coordinada para dar respuesta rápidamente a los incidentes y para reducir el impacto de los fallos de seguridad. Todos los incidentes serán reportados con posterioridad al incidente tan pronto como sea posible.

### **Procedimientos operacionales y responsabilidades**

- h) Las operaciones de seguridad de la AC serán separadas de las operaciones normales

## **6.8.2.4 Gestión del sistema de acceso**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas. En particular:

### **AC General**

- a) Se implementarán controles (p. Ej. Cortafuegos) para proteger la red interna de redes externas accesibles por terceras partes.
- b) Los datos sensibles serán protegidos cuando estos sean transmitidos por redes no protegidas.
- c) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de usuarios (incluyendo operadores, administradores y cualquier usuario que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de usuarios, auditorías y modificación o supresión inmediata de accesos.
- d) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso a la información y a las funciones del sistema está restringido de acuerdo con la política de control de accesos, y que el sistema de la AC dispone de los controles de seguridad suficientes para la separación de los roles de confianza identificados en la CPS, incluyendo la separación del administrador de seguridad y las funciones operacionales. Concretamente, el uso de utilidades del sistema estará restringido y estrictamente controlado.

- e) El personal de la AC identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de certificados.
- f) El personal de la AC será responsable de sus actos, por ejemplo, por retener logs de eventos.
- g) Se protegerán los datos sensibles contra medios de almacenamiento susceptibles de que la información sea recuperada y accesible por personas no autorizadas.

### **Generación del certificado**

- h) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los componentes de la red local (p. ej. routers) están guardados en un medio físico seguro y sus configuraciones son periódicamente auditadas
- i) Las instalaciones de la AC estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

### **Gestión de la revocación**

- j) Las instalaciones de la AC estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

#### **6.8.2.5 Gestión del ciclo de vida del hardware criptográfico**

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

- a) El hardware criptográfico de firma de certificados no se manipula durante su transporte
- b) El hardware criptográfico de firma de certificados no se manipula mientras está almacenado
- c) El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
- d) El hardware criptográfico de firma de certificados está funcionando correctamente; y;
- e) La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo

#### **6.8.3 Evaluación de la seguridad del ciclo de vida**

La evaluación de la seguridad del ciclo de vida está supeditada a la metodología interna de la AC.

### **6.9. Controles de seguridad de la red**

Camerfirma protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL.

### ***6.10. Controles de ingeniería de los módulos criptográficos***

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

## **7. Perfiles de Certificado y CRL**

### **7.1. Perfil de Certificado**

Todos los certificados emitidos bajo esta política serán conformes a:

- Estándar X.509 versión 3
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL profile”.

Y aquellos que son cualificados con:

- ETSI EN 319 412-3 v1.1.1 “Certificate Profiles-Part 2 Certificate profile for certificates issued to legal persons”

#### **7.1.1 Número de versión**

Deberá indicarse en el campo versión que se trata de la v.3

#### **7.1.2 Extensiones del certificado**

El perfil del certificado está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.

#### **7.1.3 Extensión con las facultades de representación especial.**

El certificado, emitido bajo la presente Política, incluirá una extensión en la que el solicitante detallara las facultades que le han sido otorgadas mediante poder notarial especial para la realización de determinados trámites en nombre y representación de la entidad.

#### **7.1.4 Extensiones específicas**

El certificado, emitido bajo la presente Política, podrá incluir por petición del Suscriptor extensiones adicionales con información específica de su propiedad. Esta información estará bajo la exclusiva responsabilidad del Suscriptor. Dichas extensiones no se marcarán como críticas y sean reconocibles como tales

### **7.1.5 Identificadores de objeto (OID) de los algoritmos**

Identificadores de objeto (OID) de los algoritmos criptográficos:

SHA-1 With RSA Encryption (1.2.840.113549.1.1.5)

SHA-256 With RSA Encryption (1.2.840.113549.1.1.11)

### **7.1.6 Formato de nombres**

No estipulado

### **7.1.7 Restricciones de los nombres**

No estipulado

## ***7.2. Perfil de CRL y extensiones***

Se soporta y se utilizan CRLs conformes al estándar X.509.

## ***7.3. OCSP Profile***

### **7.3.1 Número de versión**

Los certificados de respondedor OCSP son emitidos por cada AC gestionada por AC Camerfirma según el estándar RFC 6960.

### **7.3.2 Extensiones OCSP**

El perfil del certificado de OCSP está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite.



## **8. Especificación de la Administración**

### ***8.1. Autoridad de las políticas***

El departamento jurídico constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas

### ***8.2. Procedimientos de especificación de cambios***

Cualquier elemento de esta política es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la web de Camerfirma.

En la web de Camerfirma se mantendrá un histórico con las versiones anteriores de las políticas.

Los Partes usuarias afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

Si un cambio en la política afecta de manera relevante a un número significativo de Partes usuarias de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

### ***8.3. Publicación y copia de la política***

Una copia de esta política estará disponible en formato electrónico en una dirección de Internet definida en la CPS.

### ***8.4. Procedimientos de aprobación de la CPS***

Para la aprobación y autorización de una AC se deberán respetar los procedimientos especificados por la PA. Las partes de la CPS de una AC que contenga información relevante en relación a su seguridad, toda o parte de esa CPS no estarán disponible públicamente.

## Anexo I. Acrónimos

<b>AC</b>	Autoridad de Certificación
<b>AR</b>	Autoridad de Registro
<b>CPS</b>	<i>Certification Practice Statement.</i> Declaración de Prácticas de Certificación
<b>CRL</b>	<i>Certificate Revocation List.</i> Lista de certificados revocados
<b>CSR</b>	<i>Certificate Signing Request.</i> Petición de firma de certificado
<b>DES</b>	<i>Data Encryption Standard.</i> Estándar de cifrado de datos
<b>DN</b>	<i>Distinguished Name.</i> Nombre distintivo dentro del certificado digital
<b>DSA</b>	<i>Digital Signature Algorithm.</i> Estándar de algoritmo de firma
<b>DSCF</b>	Dispositivo seguro de creación de firma
<b>DSADCF</b>	Dispositivo seguro de almacén de datos de creación de firma
<b>FIPS</b>	<i>Federal Information Processing Standard Publication</i>
<b>IETF</b>	<i>Internet Engineering Task Force</i>
<b>ISO</b>	<i>International Organization for Standardization.</i> Organismo Internacional de Estandarización
<b>ITU</b>	<i>International Telecommunications Union.</i> Unión Internacional de Telecomunicaciones
<b>LDAP</b>	<i>Lightweight Directory Access Protocol.</i> Protocolo de acceso a directorios
<b>OCSP</b>	<i>On-line Certificate Status Protocol.</i> Protocolo de acceso al estado de los certificados
<b>OID</b>	<i>Object Identifier.</i> Identificador de objeto
<b>PA</b>	<i>Policy Authority.</i> Autoridad de Políticas
<b>PC</b>	Política de Certificación
<b>PIN</b>	<i>Personal Identification Number.</i> Número de identificación personal
<b>PKI</b>	<i>Public Key Infrastructure.</i> Infraestructura de clave pública

<b>RSA</b>	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
<b>SHA-1</b>	<i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash
<b>SSL</b>	<i>Secure Sockets Layer</i> . Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
<b>TCP/IP</b>	<i>Transmission Control Protocol/Internet Protocol</i> . Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

## Anexo II. Definiciones

<b>Autoridad de Certificación</b>	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y la Parte usuaria, vinculando una determinada clave pública con una persona.
<b>Autoridad de políticas</b>	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y CPS.
<b>Autoridad de Registro</b>	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
<b>Certificación cruzada</b>	El establecimiento de una relación de confianza entre dos AC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
<b>Certificado</b>	Archivo que asocia la clave pública con algunos datos identificativos del Suscriptor y es firmada por la AC.
<b>Clave pública</b>	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada <b>datos de verificación de firma</b> .
<b>Clave privada</b>	Valor matemático conocido únicamente por el Suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada <b>datos de creación de firma</b> .  La clave privada de la AC será usada para firma de certificados y firma de CRL's
<b>CPS</b>	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.

<b>CRL</b>	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
<b>Datos de Activación</b>	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
<b>DSADCF</b>	<i>Dispositivo seguro de almacén de los datos de creación de firma.</i> Elemento software o hardware empleado para custodiar la clave privada del Suscriptor de forma que solo él tenga el control sobre la misma.
<b>DSCF</b>	<i>Dispositivo Seguro de creación de firma.</i> Elemento software o hardware empleado por el Suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Suscriptor.
<b>Entidad</b>	Dentro del contexto de las políticas de certificación de Camerfirma, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el Suscriptor.
<b>Firma digital</b>	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: <ul style="list-style-type: none"> <li>a) que los datos no han sido modificados (integridad)</li> <li>b) que la persona que firma los datos es quien dice ser (identificación)</li> <li>c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)</li> </ul>
<b>OID</b>	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
<b>Par de claves</b>	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
<b>PKI</b>	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que

componen un sistema basado en la creación y gestión de certificados de clave pública.

**Política de certificación**

Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes

**Suscriptor**

Dentro del contexto de las políticas de certificación de Camerfirma, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales. Se trata del “creador del sello”.

**Parte usuaria**

Dentro del contexto de las políticas de certificación de Camerfirma, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado