POLÍTICA DE CERTIFICACIÓN

Camerfirma

Certificado Digital

CERTIFICADO DE REPRESENTANTE PARA ADMINISTRACIONES PÚBLICAS

Versión 1.1

Firmado digitalmente por: FRANCE MARIE SYLVIA VIDAL LECA
Fecha y hora: 03.10.2018 19:43:08

Información sobre el documento

Nombre:	Política de Certificación del Certificado Representante para Administraciones Públicas
Código	[PC-EIDAS-PR-AAPP]
Versión:	1.1
Elaborado por:	AC Camerfirma SA
Idioma:	Castellano
Descripción:	Define los criterios básicos a seguir por la CA que emita este tipo de certificados, por las RA's que pudiera utilizar y por Firmantes y Partes usuarias que confían de este tipo de certificados.
Fecha de edición:	Mayo 2016
Estado del documento:	Activo
Referencia (OID):	1.3.6.1.4.1.17326.10.16.1.3
Localización:	https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	PUBLICACIÓN
1.0	Creación del documento	11/05/2016
1.1	Revisión periódica. Ajustes menores CPS	Septiembre 2018

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 de algunas características especiales. En concreto, para este tipo de certificados distinguimos dentro del tipo genérico de certificados 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 Firmante o el prestador de servicios).

Ver 1.3 Identificación.

Índice de Contenido

1. Introducción *10*

1.1. Consideración Inicial **10**

1.2. Vista General **11**

1.3. Identificación **12**

1.4. Comunidad y Ámbito de Aplicación **12**

1.4.1 Autoridad de Certificación (AC) 12

1.4.2 Autoridad de Registro (AR) 13

1.4.3 Firmante 13

1.4.4 Parte usuaria 13

1.4.5 Solicitante 13

1.4.6 Entidad 13

1.4.7 Ámbito de Aplicación y Usos 13

1.4.7.1 Usos Prohibidos y no Autorizados 14

1.5. Contacto **15**

2. Cláusulas Generales *16*

2.1. Obligaciones **16**

2.1.1 AC 16

2.1.2 AR 17

2.1.3 Solicitante 17

2.1.4 Firmante 17

2.1.5 Parte usuaria 18

2.1.6 Entidad 18

2.1.7 Repositorio 18

2.2. Responsabilidad **18**

2.2.1 Exoneración de responsabilidad 19

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones 20

2.3. Responsabilidad financiera **20**

2.4. Interpretación y ejecución **20**

2.4.1 Legislación 20

2.4.2 Independencia 20

2.4.3 Notificación 20

2.4.4 Procedimiento de resolución de disputas 20

2.5. Tarifas **21**

2.5.1 Tarifas de emisión de certificados y renovación 21

2.5.2 Tarifas de acceso a los certificados 21

2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados 21

2.5.4 Tarifas por el acceso al contenido de estas Políticas de Certificación 21

2.5.5 Política de reintegros 21

2.6. Publicación y repositorios **21**

2.6.1 Publicación de información de la AC 21
2.6.1.1 Políticas y Prácticas de Certificación 21
2.6.1.2 Términos y condiciones 22
2.6.1.3 Difusión de los certificados 22
2.6.2 Frecuencia de publicación 22
2.6.3 Controles de acceso 22
2.7. Auditorias 23
2.7.1 Frecuencia de las auditorias 23
2.7.2 Identificación y calificación del auditor 23
2.7.3 Relación entre el auditor y la AC 23
2.7.4 Tópicos cubiertos por la auditoria 23
2.7.5 Auditoria en las Autoridades de Registro 23
2.8. Confidencialidad 23
2.8.1 Tipo de información a mantener confidencial 23
2.8.2 Tipo de información considerada no confidencial 24
2.8.3 Divulgación de información de revocación / suspensión de certificados 24
2.8.4 Envío a la Autoridad Competente 24
2.9. Derechos de propiedad intelectual 24
3. Identificación y Autenticación 25
3.1. Registro inicial 25
3.1.1 Tipos de nombres 25
3.1.2 Pseudónimos 25
3.1.3 Reglas utilizadas para interpretar varios formatos de nombres 25
3.1.4 Unicidad de los nombres 25
3.1.5 Procedimiento de resolución de disputas de nombres 25
3.1.6 Reconocimiento, autenticación y función de las marcas registradas 26
3.1.7 Métodos de prueba de la posesión de la clave privada 26
3.1.8 Autenticación de la identidad de una Entidad 26
3.1.9 Autenticación de la identidad de una persona física 26
3.1.9.1 Modelo orientativo de poderes 27
3.1.10 Procedimiento simplificado de emisión de certificados 27
3.1.11 Requerimientos aplicables a las AR's externas 27
3.2. Renovación de la clave y del certificado 28
3.3. Modificación de certificados 28
3.4. Reemisión después de una revocación 28
3.5. Solicitud de revocación 28
4. Requerimientos Operacionales 29
4.1. Solicitud de certificados 29
4.2. Petición de certificación cruzada 30
4.3. Emisión de certificados 30
4.4. Aceptación de certificados 31
4.5. Suspensión y revocación de certificados 31
4.5.1 Aclaraciones previas 31
4.5.2 Causas de revocación 32

4.5.3 Quién puede solicitar la revocación 33
4.5.4 Procedimiento de solicitud de revocación 33
4.5.5 Periodo de revocación 34
4.5.6 Suspensión 34
4.5.7 Procedimiento para la solicitud de suspensión 34
4.5.8 Límites del periodo de suspensión 34
4.5.9 Frecuencia de emisión de CRL's 34
4.5.10 Requisitos de comprobación de CRL's 34
4.5.11 Disponibilidad de comprobación on-line de la revocación 35
4.5.12 Requisitos de la comprobación on-line de la revocación 35
4.5.13 Otras formas de divulgación de información de revocación disponibles 35
4.5.14 Requisitos de comprobación para otras formas de divulgación de información de revocación 35
4.5.15 Requisitos especiales de revocación por compromiso de las claves 35

4.6. Procedimientos de Control de Seguridad 35
4.6.1 Tipos de eventos registrados 37
4.6.2 Frecuencia de procesado de Logs 38
4.6.3 Periodos de retención para los Logs de auditoria 38
4.6.4 Protección de los Logs de auditoría 38
4.6.5 Procedimientos de backup de los Logs de auditoría 38
4.6.6 Sistema de recogida de información de auditoria 38
4.6.7 Notificación al sujeto causa del evento 38
4.6.8 Análisis de vulnerabilidades 39

4.7. Archivo de registros 39
4.7.1 Tipo de archivos registrados 39
4.7.2 Periodo de retención para el archivo 39
4.7.3 Protección del archivo 39
4.7.4 Procedimientos de backup del archivo 40
4.7.5 Requerimientos para el sellado de tiempo de los registros 40
4.7.6 Sistema de recogida de información de auditoria 40
4.7.7 Procedimientos para obtener y verificar información archivada 40

4.8. Cambio de clave de la AC 40

4.9. Recuperación en caso de compromiso de la clave o desastre 40
4.9.1 La clave de la AC se compromete 41
4.9.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre 41

4.10. Cese de la AC 41

5. Controles de Seguridad Física, Procedimental y de Personal 43

5.1. Controles de Seguridad física 43
5.1.1 Ubicación y construcción 44
5.1.2 Acceso físico 44
5.1.3 Alimentación eléctrica y aire acondicionado 44
5.1.4 Exposición al agua 44
5.1.5 Protección y prevención de incendios 44
5.1.6 Sistema de almacenamiento. 44
5.1.7 Eliminación de residuos 44
5.1.8 Backup remoto 45

5.2. Controles procedimentales 45
5.2.1 Roles de confianza 45
5.2.2 Número de personas requeridas por tarea 45
5.2.3 Identificación y autentificación para cada rol 46

5.3. Controles de seguridad de personal 46
5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación 46
5.3.2 Procedimientos de comprobación de antecedentes 47
5.3.3 Requerimientos de formación 47
5.3.4 Requerimientos y frecuencia de la actualización de la formación 47
5.3.5 Frecuencia y secuencia de rotación de tareas 47
5.3.6 Sanciones por acciones no autorizadas 47
5.3.7 Requerimientos de contratación de personal 47
5.3.8 Documentación proporcionada al personal 48

6. Controles de Seguridad Técnica 49

6.1. Generación e instalación del par de claves 49
6.1.1 Generación del par de claves de la AC 49
6.1.2 Generación del par de claves del Firmante 49
6.1.3 Entrega de la clave privada al Firmante 49
6.1.4 Entrega de la clave pública del Firmante al emisor del certificado 50
6.1.5 Entrega de la clave pública de la CA a las Partes usuarias 50
6.1.6 Tamaño y periodo de validez de las claves del emisor 50
6.1.7 Tamaño y periodo de validez de las claves del Firmante 51
6.1.8 Parámetros de generación de la clave pública 51
6.1.9 Comprobación de la calidad de los parámetros 51
6.1.10 Hardware/software de generación de claves 51
6.1.11 Fines del uso de la clave 51

6.2. Protección de la clave privada 52

6.3. Estándares para los módulos criptográficos 52
6.3.1 Control multipersona (n de entre m) de la clave privada 52
6.3.2 Depósito de la clave privada (key escrow) 53
6.3.3 Copia de seguridad de la clave privada 53
6.3.4 Archivo de la clave privada 53
6.3.5 Introducción de la clave privada en el módulo criptográfico 53
6.3.6 Método de activación de la clave privada 53
6.3.7 Método de desactivación de la clave privada 54
6.3.8 Método de destrucción de la clave privada 54

6.4. Otros aspectos de la gestión del par de claves 54
6.4.1 Archivo de la clave pública 54
6.4.2 Periodo de uso para las claves públicas y privadas 54

6.5. Datos de activación 54
6.5.1 Generación y activación de los datos de activación 54
6.5.2 Protección de los datos de activación 54
6.5.3 Otros aspectos de los datos de activación 55

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) 55

6.7. Controles de seguridad informática 55
6.7.1 Requerimientos técnicos de seguridad informática específicos 56
6.7.2 Valoración de la seguridad informática 56

6.8. Controles de seguridad del ciclo de vida 56
6.8.1 Controles de desarrollo del sistema 56
6.8.2 Controles de gestión de la seguridad 56
6.8.2.1 Gestión de seguridad 56
6.8.2.2 Clasificación y gestión de información y bienes 57
6.8.2.3 Operaciones de gestión 57
6.8.2.4 Gestión del sistema de acceso 58
6.8.2.5 Gestión del ciclo de vida del hardware criptográfico 59
6.8.3 Evaluación de la seguridad del ciclo de vida 59

6.9. Controles de seguridad de la red 59

6.10. Controles de ingeniería de los módulos criptográficos 60

7. Perfiles de Certificado y CRL 61

7.1. Perfil de Certificado 61
7.1.1 Número de versión 61
7.1.2 Extensiones del certificado 61
7.1.3 Extensión con las facultades de representación especial. 61
7.1.4 Extensiones específicas 61
7.1.5 Identificadores de objeto (OID) de los algoritmos 61
7.1.6 Formato de nombres 62
7.1.7 Restricciones de los nombres 62

7.2. Perfil de CRL 62
7.2.1 Número de versión 62
7.2.2 CRL y extensiones 62

7.3. OCSP Profile 62
7.3.1 Número de versión 62
7.3.2 Extensiones OCSP 62

8. Especificación de la Administración 63

8.1. Autoridad de las políticas 63

8.2. Procedimientos de especificación de cambios 63

8.3. Publicación y copia de la política 63

8.4. Procedimientos de aprobación de la CPS 63

Anexo I. Acrónimos 64

Anexo II. Definiciones 66

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, entendemos 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 Firmante o Parte usuaria que confía 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.

En caso de conflicto entre la CPS y las Políticas se tomará en cuenta lo que describa la CPS al ser un documento que describe las prácticas actualizadas del prestador. Cuando no exista un requerimiento concreto en las políticas se deja libertad al prestador para tomar las decisiones correspondientes al punto en cuestión. Las decisiones tomadas pueden ser propias del prestador o impuestas por otras normativas o políticas aplicables. Estas decisiones deben estar descritas en las prácticas de certificación, así como las políticas de certificación aplicables siendo esta una de ellas.

1.2. Vista General

El presente documento especifica la Política de Certificación del Certificado de Representante para Administraciones Públicas en base a las políticas definidas por el Ministerio de Hacienda y Administraciones Públicas en si versión 2.0.

Esta Política de Certificación está en conformidad con las disposiciones legales que rigen el asunto de Firma Electrónica en la Unión Europea y en España, cumpliendo todos los requisitos técnicos y de seguridad exigidos para emisión de certificados cualificados o reconocidos.

Esta política define las reglas y responsabilidades que deben seguir aquellas Autoridades de certificación que deseen emitir el tipo de certificado definido en el presente documento, imponiendo además ciertas obligaciones que deben ser tenidas en cuenta por los Firmantes/ y las Partes usuarias que confían en virtud de su especial relación con este tipo de certificados.

De esta forma, cualquier AC que emita este tipo de certificados, deberá ajustarse a los niveles de seguridad que se detallan en esta política de certificación y deberán informar a sus Firmantes de su existencia.

Los certificados emitidos bajo esta política requerirán la autenticación de la identidad de los Firmantes. Esta identificación y autentificación se realizará según los términos de esta política.

La AC suspenderá y 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.

Las claves de los Firmantes tienen un periodo de validez determinado por esta política y en ningún caso podrán realizarse copias de back-up, ni almacenarse por la AC.

La información personal recabada del Firmante 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 vigente en cada momento.

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) hay algunas informaciones útiles.

1.3. Identificación

Certificado	OID Política
Certificado Cualificado de Representante de Persona Jurídica para trámites con las AAPP en QSCD	[Camerfirma] 1.3.6.1.4.1.17326.10.16.1.3.2.1 [normativa nacional] 2.16.724.1.3.5.8 [ETSI EN 319 411 2 - QCP-n-qscd] 0.4.0.194112.1.2
Certificado Cualificado de Representante de Persona Jurídica para trámites con las AAPP	[Camerfirma] 1.3.6.1.4.1.17326.10.16.1.3.2.2 [normativa nacional] 2.16.724.1.3.5.8 [ETSI EN 319 411 2 - QCP-n] 0.4.0.194112.1.0
Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica para trámites con las AAPP en QSCD	[Camerfirma] 1.3.6.1.4.1.17326.10.16.1.3.2.1 [normativa nacional] 2.16.724.1.3.5.9 [ETSI EN 319 411 2 - QCP-n-qscd] 0.4.0.194112.1.2
Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica para trámites con las AAPP	[Camerfirma] 1.3.6.1.4.1.17326.10.16.1.3.2.2 [normativa nacional] 2.16.724.1.3.5.9 [ETSI EN 319 411 2 - QCP-n] 0.4.0.194112.1.0

1.4. Comunidad y Ámbito de Aplicación

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 Firmante y la Parte usuaria que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona (Firmante) relacionada a una entidad concreta (Persona Jurídica o Entidad sin Personalidad Jurídica), a través de la emisión de un Certificado.

El emisor de este tipo de certificados es AC Camerfirma SA.

1.4.2 Autoridad de Registro (AR)

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la AC, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

1.4.3 Firmante

Bajo esta Política el Firmante es una persona física, representante de una determinada entidad (Persona Jurídica o Entidad sin Personalidad Jurídica), poseedor de un dispositivo de creación de firma con un Certificado emitido bajo esta política.

1.4.4 Parte usuaria

En esta Política se entiende por Parte usuaria la persona física o jurídica que voluntariamente confía en el certificado emitido a favor del emisor, lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado y en consecuencia se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

1.4.5 Solicitante

Se entenderá por Solicitante la persona física que solicita el Certificado. A efectos de esta Política, la figura del Solicitante coincide con la figura del Firmante.

Podrán solicitar el certificado de representante para las Administraciones Públicas: los representantes legales de la Entidad, los apoderados generales y los apoderados voluntarios con poder especial bastante a estos efectos.

1.4.6 Entidad

A efectos de la presente Política de Certificación nos referiremos a una Entidad como aquella empresa u organización de cualquier tipo, con o sin personalidad jurídica, representada por el Firmante .

La Entidad deberá solicitar la suspensión / revocación del certificado cuando cese la capacidad de representación que ostenta el Firmante.

1.4.7 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política, permite identificar al representante de una Entidad, y acreditar su relación de representación bastante para actuar en nombre de ésta ante las Administraciones PúblicasR4.

El Certificado emitido bajo esta Política puede ser utilizado con los siguientes propósitos:

Identificación del Firmante y de su relación de representación de la Entidad: El Firmante del Certificado puede autenticar, frente a otra parte, su identidad y su relación de representación de una Entidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.

El Firmante podrá identificarse válidamente ante las Administraciones Públicas y vincular a la Entidad mediante la firma de cualquier documento o dato.

Integridad del documento firmado: La utilización de este Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de haber sido firmado por el Firmante. Se certifica que el mensaje recibido por la Parte usuaria es el mismo que fue emitido por el Firmante

No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Firmante que ha firmado no puede negar la autoría o la integridad del mismo.

A pesar de ser posible su utilización para el cifrado de datos, la AC no se responsabiliza por esta actividad, debido a que, por motivos de seguridad, esta Política determina que la AC no guarde copia de la clave privada del Firmante. No se garantiza, por tanto, la recuperación de los datos cifrados en caso de pérdida de la clave privada por parte del Firmante, el Firmante o la Parte usuaria lo hará, en todo caso, bajo su propia responsabilidad.

1.4.7.1 Usos Prohibidos y no Autorizados

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso.

El empleo de los certificados que implique la realización de operaciones no autorizadas según las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los Contratos de la AC con sus Firmantes tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el Firmante o cualquier tercero.

En función de los servicios prestados por la AC mediante la emisión de sus certificados, no es posible por parte de la AC el acceso o conocimiento del contenido del mensaje al que haya sido adjuntado o con el que se relacione el uso de un certificado emitido por la AC.

Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la AC emitir valoración alguna sobre dicho contenido, asumiendo por tanto el Firmante cualquier responsabilidad dimanante del contenido de dicho mensaje aparejado al uso de un certificado emitido por la AC. Asimismo, le será imputable al Firmante cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las

Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los contratos de la AC con sus Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5. Contacto

La presente política de certificación, está administrada y gestionada por el Departamento Jurídico de AC Camerfirma SA, pudiendo ser contactado por los siguientes medios:

E-mail:	juridico@camerfirma.com
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 y libres de errores de entrada de datos
5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados cualificados.
6. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
7. Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL
8. Informar a los Firmantes de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
9. Publicar esta Política y las Prácticas correspondientes en su página web.
10. Informar sobre las modificaciones de esta Política y de su CPS a los Subscriptores y AR's que estén vinculadas a ella.
11. No almacenar ni copiar los datos de creación de firma del Firmante, en caso de su gestión en nombre de éste.
12. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
13. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante perdida o destrucción o falsificación
14. 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.
4. Verificar la exactitud y autenticidad de la información suministrada por el Firmante/Solicitante.
5. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Firmante.
6. Respetar lo dispuesto en los contratos firmados con la AC y con el Firmante.
7. Informar a la AC las causas de revocación, siempre y cuando tomen conocimiento.

2.1.3 Solicitante

El Solicitante de un Certificado deberá cumplir con lo dispuesto por la normativa aplicable y además deberá:

1. Suministrar a la AR la información necesaria para realizar una correcta identificación del Firmante y de la Entidad.
2. Demostrar ser poseedor de facultades de representación legal o poderes generales o poderes especiales que le permiten actuar en nombre de la Entidad en cualquier actuación administrativa con las Administraciones Públicas. , vigentes.
3. 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 Firmante

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

1. Custodiar su clave privada de manera diligente.
2. Usar el certificado según lo establecido en la presente Política de Certificación.
3. Respectar lo dispuesto en contrato firmado con la Autoridad de Certificación.

4. Informar de la existencia de alguna causa de suspensión /revocación.

5. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

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 Entidad

Será obligación de la Entidad solicitar a la AR la suspensión / revocación del certificado cuando cese la capacidad de representación que ostenta el Firmante.

2.1.7 Repositorio

La información relativa a la publicación y revocación /suspensión 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 Firmante 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, en el momento de la entrega del certificado, obra en poder del responsable de la entidad, la clave privada correspondiente a la clave pública dada o identificada en el certificado

3. la garantía de que la clave pública y privada funcionan conjunta y complementariamente

4. la correspondencia entre el certificado solicitado y el certificado entregado

5. Cualquier responsabilidad que se establezca por la legislación vigente.

2.2.1 Exoneración de responsabilidad

Las ACs y las ARs 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 CRLs emitidos por la Autoridad de Certificación

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 Firmante, el Responsable de la Entidad o Partes usuarias 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 /suspensión.

7. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.

8. Por la no recuperación de documentos cifrados con la clave pública del Firmante.

9. Fraude en la documentación presentada por el Solicitante

10. La AC no se responsabiliza del contenido ni del alcance de las facultades o de los poderes del representante de la Entidad, Firmante del certificado.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

Independientemente del importe de las transacciones, este tipo de certificados tienen un límite de responsabilidad igual a 0 €.

Esta garantía será de aplicación a efectos de lo dispuesto en la legislación vigente.

2.3. Responsabilidad financiera

La AC no asume ningún tipo de responsabilidad financiera.

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 vigente 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 cualesquiera otros servicios relacionados estarán disponibles para las Partes usuarias en la página web de Camerfirma www.camerfirma.com y / o en la de cada AR concreta.

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 las Partes usuarias en la dirección de Internet http://www.camerfirma.com y / o en la de cada AR concreta.

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 encuentra disponible en el sitio de Internet en la dirección de Internet http://www.camerfirma.com.

Las Prácticas de Certificación de referencia serán así mismo públicas y se pondrán a disposición del público en la dirección de Internet http://www.camerfirma.com .

2.6.1.2 Términos y condiciones

La AC o la AR pondrá a disposición de los Firmantes y Partes usuarias los términos y condiciones del servicio antes de proceder a la emisión del certificado o de entregar los PINES o claves que permitan el acceso a la clave privada.

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 Firmantes y Partes usuarias.

En concreto:

a) El certificado de la AC es público y se encontrará disponible en la página web de Camerfirma www.camerfirma.com.

b) El resto de los certificados estarán disponibles al público en la página web de Camerfirma sólo en los casos en que el Firmante 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 refieren los puntos a) y b) 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 AC publicará los certificados suspendidos en el momento en que reciba una petición autenticada y existan indicios de su necesidad.

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 Firmantes 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 a 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 auditoria

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.

2.7.5 Auditoria en las Autoridades de Registro

Todas las Autoridades de Registro deben ser auditadas al ser estas entidades delegadas de actividades responsabilidad de la AC. Estas auditorías se realizarán como mínimo cada dos años y podrán ser realizadas por la propia AC o por una entidad externa.

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 totalidad de la normativa vigente en materia de protección de datos.

La AC pondrá todos los medios a su alcance para garantizar la confidencialidad frente a terceros, durante el proceso de generación, de las claves privadas de firma digital que proporciona. Asimismo, una vez generadas y entregadas las claves privadas, la AC se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves.

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 Firmante 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 / suspensión de certificados

La forma de difundir la información relativa a la suspensión o 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 de la Parte usuaria de forma legítima 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 Firmantes requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

3.1.2 Pseudónimos

Los pseudónimos no serán admitidos.

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.

Se permite el uso dentro del CN del uso de un ACRÓNIMO que identifique a la Entidad a la que está vinculado el Firmante del certificado. Esta alternativa es importante cuando un Firmante posee más de un certificado debido a su vinculación a más de una Entidad. Algunos aplicativos solo muestran el nombre del Firmante a la hora de elegir un certificado del almacén para realizar un proceso de autenticación o firma. En estos casos el Firmante no tiene una forma rápida de diferenciar el certificado a usar.

El formato del CN dentro del certificado será:

"Nombre del Firmante [ACRONIMO]"

3.1.4 Unicidad de los nombres

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los certificados emitidos. El atributo del SerialNumber se usará para distinguir entre dos DN's similares. La AC es responsable de realizar los esfuerzos que razonablemente estén a su alcance para asegurar que el SerialNumber es suficiente para resolver las posibles colisiones entre nombres.

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 admitirá la identificación de marcas o acrónimos de entidades siempre que en el propio certificado aparezca, además, la razón social y el número de identificación fiscal de la Entidad, titular del signo distintivo registrado o no. 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

Si el par de claves es generado por el Firmanter, la AC proveerá en la CPS la garantía de estar en posesión de clave privada. En caso contrario, la AC deberá tomar las medidas necesarias que aseguren que el Firmante está en posesión de la clave privada asociada a la clave pública.

3.1.8 Autenticación de la identidad de una Entidad

Los Certificados emitidos bajo la presente Política identifican a una persona física que actúa como representante de la Entidad, por lo que se exigirá, en todo caso, la acreditación de la existencia de la Entidad por un medio conforme a Derecho.

3.1.9 Autenticación de la identidad de una persona física

Para realizar una correcta identificación de la identidad del Solicitante/Firmante, se deberá atender a lo dispuesto por la legislación vigente.

Para los certificados emitidos bajo esta Política se exige, además, la comprobación de que el Firmante tiene la capacidad de representar a la Entidad ante las Administraciones Públicas por su condición de representante legal o voluntario (poderes generales o poderes específicos para actuar ante las AAPP).

Para la mencionada comprobación de la identidad del Solicitante se exigirá la presencia física del Firmante y la entrega de la copia y del original (para su cotejo) de la Escritura de elevación a público del nombramiento del representante legal o de los Poderes Generales o del Poder especial para actuar ante las AAPP (o del documento legal correspondiente de designación de representante o apoderadoen caso de entidades sin personalidad jurídica).

Este requisito de presencia física podrá eximirse en dos casos:

a) Cuando el solicitante se identifique de forma telemática mediante otro certificado reconocido o cualificado para cuya entrega se haya requerido presencia física y la verificación de los poderes.

b) Cuando sea presentado por otra persona a la que previamente haya autorizado el Firmante y siempre que su firma en la autorización haya sido legitimada notarialmente.

3.1.9.1 Modelo orientativo de poderes

La AR deberá verificar que el Firmante dispone de facultades de representación generales (representante legal o representante voluntario con poderes generales) para actuar en nombre de la Entidad a la que representa o por lo menos de poderes especiales para actuar ante las AAPP. No obstante lo anterior, el contenido y alcance concreto de dichos poderes deberá ser verificado por la Parte usuaria antes de depositar su confianza en el certificado, en función del negocio jurídico subyacente en la transacción electrónica.

A efectos de la emisión de este tipo de certificados se darán por válidos los poderes de los representantes legales, los poderes generales de representante voluntarios y los poderes especiales que contengan al menos un párrafo del siguiente tenor: "solicitar certificados electrónicos para la representación de la [entidad] para la realización de firma electrónica en cualquier actuación administrativa con las Administraciones Públicas que requiera del uso de la firma electrónica o del certificado"

3.1.10 Procedimiento simplificado de emisión de certificados

Se establecerá un procedimiento especial de registro simplificado para los casos en los que deba solicitarse un nuevo certificado por el cambio de alguno de los datos presentados por el Firmante respecto de una solicitud anterior.

El Firmante asumirá la responsabilidad mediante declaración firmada de la corrección de los datos no modificados.

La AR únicamente deberá comprobar la documentación que en su caso deba presentar el Firmante respecto de los datos cuya modificación ha declarado.

3.1.11 Requerimientos aplicables a las AR's externas

Cuando la AC emplee AR's externas deberá asegurar los siguientes aspectos:

- Que la identidad de la AR y de los administradores de la AR ha sido correctamente comprobada y validada.
- Que los administradores de la AR han recibido formación suficiente para el desempeño de sus funciones.
- Que la AR está autorizada para realizar las funciones de registro.
- Que la AR ha sido auditada por la AC o por una entidad externa.
- Que la AR asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.

- Que la comunicación entre la AR y la AC, se realiza de forma segura mediante el uso de certificados digitales.

3.2. Renovación de la clave y del certificado

La AC deberá informar al Firmante 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 usando la anterior clave pública del Firmante.

Un certificado podrá ser renovado un máximo de tres veces, 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.

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 .

4. Requerimientos Operacionales

4.1. Solicitud de certificados

La AC se asegurará de que los Firmantes están correctamente identificados y autorizados y que la petición del certificado es completa.

Registro

a) Antes de comenzar una relación contractual, la AC, por sí misma o por medio de la AR, deberá informar al Solicitante de los términos y condiciones relativos al uso del certificado

b) Se deberá comunicar esta información a través de un medio de comunicación perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

c) La AC, por sí misma o por medio de la AR, deberá comprobar, de acuerdo con la legislación vigente, la identidad y los atributos específicos del Firmante. La comprobación de la identidad del Firmante se realizará mediante la personación física del mismo y la exhibición por éste del DNI, pasaporte, tarjeta de residencia o documento equivalente o mediante otro certificado según lo dispuesto en el apartado 3.1.9.

d) Se registrará en todo caso:

- Nombre completo del Firmante.
- Número del DNI, pasaporte o tarjeta de residencia del Firmante.
- Nombre completo y forma jurídica de la Entidad.
- Evidencia de la existencia de la Entidad.
- Evidencia de los poderes) del Firmante para representar a la Entidad.

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

f) La AC deberá registrar toda la información usada para comprobar la identidad de los Firmantes, incluyendo cualquier número de referencia en la documentación empleada para la verificación y los límites de su validez.

g) La AC deberá guardar el contrato firmado con el Firmante, el cual incluirá:

- Acuerdo de las obligaciones del Firmante.
- Compromiso del Firmante a usar el dispositivo de creación de firma ofrecido por la AC de forma diligente.

- Consentimiento para que la AC guarde la información usada para el registro, entrega del dispositivo del Firmante, para una futura revocación, así como para el traspaso de información a una tercera parte en el caso de que la AC cese su actividad.

- Si y bajo qué condiciones el Firmante consiente la publicación del certificado

- Que la información contenida en el certificado es correcta

h) Los registros identificados deberán conservarse durante el periodo de tiempo que se indicó al Firmante y que es necesario a efectos probatorios en los procedimientos legales.

i) Si el par de claves no es generado por la AC, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el Firmante está en posesión de la clave privada asociada a la clave pública.

j) 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:

- Cuando la AC genere las claves del Firmante, que el procedimiento de emisión del certificado está ligado de manera segura a la generación del par de claves por la AC

- Cuando la AC no genere las claves del Firmante, que la clave privada o el dispositivo seguro de creación de firma ha sido generado de manera segura por el Firmante.

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

- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Firmante 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 deberá notificar al solicitante la emisión de su certificado.

4.4. Aceptación de certificados

La entrega del certificado y la firma del contrato de adhesión al sistema de certificación implicará la aceptación del certificado por parte del Firmante.

La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el encargado de la AC o AR. El Solicitante emitirá esta aceptación en su propio nombre.

No obstante, a partir de la entrega del certificado, existirá 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 Firmante en el caso de que la diferencia entre los datos sea causada por un error no imputable al Firmante. Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el Firmante ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, se confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AR, 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 Aclaraciones previas

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de un certificado en función de alguna circunstancia distinta a la caducidad del mismo. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

La suspensión por su parte supone una revocación con causa de suspensión, esto es, se revoca un certificado temporalmente hasta que se decida sobre la oportunidad o no de realizar una revocación definitiva.

Por tanto, a efectos de la presente política de certificación, hablaremos de revocación para referirnos a aquella revocación de carácter definitivo y a la suspensión como aquella revocación con causa de suspensión.

4.5.2 Causas de revocación

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

- Solicitud voluntaria del Firmante.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del Firmante o incapacidad sobrevenida, total o parcial.
- Terminación de la vinculación del Firmante con la entidad o pérdida de los poderes de representación.
- Cese en la 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 Firmante o de la AC han sido comprometidas, bien porque concurran 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 AR, AC o el Firmante de las obligaciones establecidas en esta política.
- Por la resolución del contrato con el Firmante.
- 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 extinción de la Entidad.
- Por la concurrencia de cualquier otra causa especificada en la presente política.

4.5.3 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse únicamente por el propio Firmante, la Entidad a través de su representante legal o por la propia AC.

Todas las solicitudes deberán ser en todo caso autenticadas.

4.5.4 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 todos las Partes usuarias. Este deberá ser como máximo de 3 horas

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

El Firmante cuyo certificado haya sido suspendido o revocado deberá ser informado del cambio de estado del certificado. Así mismo, el Firmante deberá ser informado del levantamiento de la suspensión. 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 (no suspendido), este no podrá volver a su estado activo. La revocación de un certificado es una acción, por tanto, definitiva.

Cuando se usen listas de certificados revocados (CRLs) que incluyan algunas variantes (p. Ej. Delta CRLs), estas serán publicadas al menos semanalmente.

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

El servicio de gestión de las revocaciones 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 no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

La información relativa al estado de la revocación estará disponible las 24 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 deberá 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.

4.5.5 Periodo de revocación

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

4.5.6 Suspensión

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

4.5.7 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.

4.5.8 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.

4.5.9 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.

4.5.10 Requisitos de comprobación de CRL's

Las Partes usuarias podrán comprobar el estado de los certificados en los cuales van 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.

4.5.11 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.

4.5.12 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.

La AC dispondrá de un sistema de consulta que impida la obtención masiva de datos relativos a los Firmantes, 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.

4.5.13 Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.5.14 Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado

4.5.15 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 las claves y 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, incluyendo la siguiente:

- La documentación presentada por el Solicitante para el registro
- Número de DNI, pasaporte o de cualquier otro documento acreditativo de la identidad del Solicitante
- Copia de documentos identificativos (DNI, pasaporte, ...), incluido el contrato suscrito con el Firmante.
- Algunas cláusulas específicas contenidas en el contrato (p.ej. el consentimiento de la publicación del certificado).
- Método empleado para comprobar la validez de los documentos identificativos, si existe
- Nombre de la Autoridad de Registro.

j) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la privacidad de la información relativa al Firmante.

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

Entrega del dispositivo al Firmante

m) La AC registrará todos los eventos relativos al ciclo de vida de las claves gestionadas por la misma, incluyendo las claves de los Firmantes generadas por la AC

Gestión de la revocación

n) 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 Firmantes/Suscriptores y actualizar
- acceso físico a los logs

- cambios en la configuración y mantenimiento del sistema
- cambios personales
- registros de la destrucción de los medios que contienen las claves, datos de activación

4.6.2 Frecuencia de procesado de Logs

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

La AC 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 auditoria

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 auditoria

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 de la auditoría
- todos los datos relativos a los certificados, incluyendo los contratos con los Firmantes/Suscriptores y los datos relativos a su identificación
- solicitudes de emisión y revocación de certificados
- todos los certificados emitidos o publicados
- CRLs emitidas o registros del estado de los certificados generados
- la documentación requerida por los auditores
- historial de claves generadas
- las comunicaciones entre los elementos de la PKI

La AC es responsable del correcto archivo de todo este material

4.7.2 Periodo de retención para el archivo

La información detallada en el apartado 4.6 h), k) y l), los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante 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 autorizada.

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.

Los siguientes certificados serán puestos a disposición pública en el directorio:

Clave pública de la nueva CA firmada por la clave privada de la vieja CA

Clave pública de la vieja CA firmada con la clave privada de la nueva CA.

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 Firmantes, 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 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 Firmantes 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 Firmantes, 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 Firmantes y Partes usuarias.
- Las claves privadas de la AC serán destruidas 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 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 Firmantes, empleados, Partes usuarias y RAs 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

a) El acceso físico a las instalaciones vinculadas a la generación de certificados, entrega del dispositivo al Firmante 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.

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

c) Se establecerán controles para evitar el compromiso o robo de información

Generación de certificados, entrega del dispositivo del Firmante y gestión de revocaciones.

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

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

f) Los controles de seguridad física y medioambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en sí 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, entrega del dispositivo del Firmante 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, ...

g) 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 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, 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 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 AC para prevenir que una persona use el sistema el sistema de AC y la clave de la AC sin detección.

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

5.2.2 Número de personas requeridas 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 autentificación 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 y AR deberá recibir los manuales de Tercero que confía en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, suspensión, 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 asegurado 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 Firmante

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

Si las claves del Firmante 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 Firmante

Cuando la clave privada del Firmante sea generada por la AC, ésta le será entregada de manera que la confidencialidad de la misma no sea comprometida y sólo el Firmante 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 confia (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 Firmante pueda generar sus propias claves, la clave pública del Firmante 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 las Partes usuarias

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 Firmantes/Suscriptores firmados con esa clave

6.1.7 Tamaño y periodo de validez de las claves del Firmante

El Firmante 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 Firmante 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

Las claves de la AC deberán ser generadas en un módulo criptográfico validado al menos por el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente

El par de claves y las claves simétricas para los Firmantes/Suscriptores serán generadas en un módulo de software y / o hardware criptográfico.

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

La clave privada del Firmante deberá ser usada únicamente para la generación de firmas electrónicas avanzadas, de acuerdo con el apartado 1.4.7.

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 regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

Del Firmante

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada está protegida de forma que:

- el Firmante o un responsable suyo pueda mantener la clave privada bajo su exclusivo control
- su secreto está razonablemente asegurado, y
- la clave privada puede ser efectivamente protegida por el Firmante o un responsable suyo contra un uso ajeno

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 multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona 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.

En ningún caso la AC podrá almacenar la clave privada de firma del Firmante, salvo en caso de su gestión por parte 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 de los Firmantes/Suscriptores se regirán 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 una vez finalizado su ciclo de vida.

Las claves privadas de Firmante no pueden ser archivadas por la AC, salvo en caso de su gestión por parte 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.

Se deberá proteger el acceso a la clave privada del Firmante por medio de un password, PIN, u otros métodos de activación equivalentes. Si estos datos de activación deben ser entregados al Firmante, esta entrega deberá realizarse por medio de un canal seguro.

Estos datos de activación deberán tener una longitud de al menos 4 dígitos en el caso de custodia en un dispositivo hardware y de 8 en el caso de dispositivo software.

Los datos de activación deben ser memorizados por el Firmante y no deben ser anotados en un lugar de fácil acceso ni compartidos.

6.3.7 Método de desactivación de la clave privada

La clave privada del Firmante podrá quedar inaccesible después de sucesivos intentos en la introducción del código de activación.

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.

Las claves privadas de los Firmantes deberán ser destruidas o hacerlas inservibles después del fin de su ciclo de vida por el propio Firmante.

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 Firmante.

f) Cuando el DSADCF o DSCF lleve asociado unos datos de activación (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 las Partes usuarias.
- controles de acceso basados en privilegios.
- control dual para ciertas operaciones relativas a la seguridad.
- generación de logs, revisión de auditoria 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 Firmante y la AC y datos de auditoria.
- auditoria 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 informática viene reflejada por un proceso de gestión de riesgos 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 con un nivel de seguridad suficiente para la funcionalidad y seguridad que se exige.

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 por el foro de gestión de CA.

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 con el 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. Firewalls) 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 Partes usuarias (incluyendo operadores, administradores y cualquier Tercero que confía que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de Partes usuarias, 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 de la AC deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-3 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".
- ETSI EN 319 412-2 v2.1.1 "Certificate Profiles-Part 2 Certificate profile for certificates issued to natural 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 se reflejará las facultades del Firmante que le han sido otorgadas mediante Escritura de elevación a público de nombramiento (representante legal), poder notarial general o poder notarial especial para actuar ante las AAPP (representante voluntario), o mediante documento legal acreditativo de la relación de representación o de apoderamiento (en caso de entidades sin personalidad jurídica) para la realización de determinados trámites en nombre y representación de la entidad ante las AAPP.

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

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

7.2.1 Número de versión

El formato de las CRLs utilizadas es el especificado en la versión 2 (X509 v2).

7.2.2 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 terceros que confían 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 terceros que confían 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

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

RSA Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado

SHA *Secure Hash Algorithm.* Algoritmo seguro de Hash

SSL *Secure Sockets Layer.* 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.

TCP/IP *Transmission Control. Protocol/Internet Protocol*. 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

Autoridad de Certificación	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Tercero que confía, vinculando una determinada clave pública con una persona.
Autoridad de políticas	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.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	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.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada **datos de verificación de firma.**
Clave privada	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada **datos de creación de firma.** La clave privada de la AC será usada para firma de certificados y firma de CRL's.
CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta..
CRL	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.

Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada.
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.
DSCF	*Dispositivo Seguro de creación de firma*. 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.
Entidad	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 firmante.
Firma digital	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: a) que los datos no han sido modificados (integridad). b) que la persona que firma los datos es quien dice ser (identificación). c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen).
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	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.
Firmante	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.
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.

Firmado digitalmente por: RAMIRO MUÑOZ MUÑOZ
Motivo: VALIDADO EXPLOTACION
Localización: AVILA
Fecha y hora: 03.10.2018 19:27:29