POLÍTICA DE CERTIFICACIÓN

CAMERFIRMA EXPRESS CORPORATE SERVER

Versión 1.1.2

Idioma: **Castellano**

Fecha: Junio **2015**

Estado del documento: **Activo**

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 Camerfirma para Camerfirma Express Corporate Server
Código	PC-SER
Versión:	1.1.2
Elaborado por:	AC Camerfirma SA
Idioma:	Castellano
Descripción:	Define los criterios básicos a seguir por la CA que emita certificados de servidor seguro para el establecimiento de canales SSL/TLS bajo protocolos HTTS, por las RA's que pudiera utilizar y por suscriptores y terceros que confían de este tipo de certificados.
Fecha de edición:	Junio 2015
Estado del documento:	Activo
Referencia (OID):	**1.3.6.1.4.1.17326.10.11.2**
Localización:	https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	PUBLICACIÓN
v1.0.1	Modificaciones del perfil del certificado. Quitamos las extensiones de Netscape, dan problemas en algunos servidores	Mayo 2007
V1.1	Ajustes de la política. Sacamos los perfiles de los certificados fuera.	Mayo 2008
v1.1.1	Revisión general y corrección de referencias erróneas entre apartados. Incluida la modificación de certificados (apartado 3.3) y la solicitud de revocación (apartado 3.5). Corrección del apartado de instalación de seguridad después de un desastre natural u otro tipo de desastre (apartado 4.9.2) Incluido el apartado referente a datos de activación (apartado 6.5) Incluida la valoración de la seguridad informática (apartado 6.7.2) Incluidos los apartados de controles de desarrollo del sistema (apartado 6.8.1), evaluación de la seguridad del ciclo de vida (apartado 6.8.3) y controles de seguridad de la red (apartado 6.9) Actualizados los apartados de los perfiles de Certificado y CRL (apartado 7) Modificada la longitud mínima de las claves del Firmante/Suscriptor (apartado 6.1.7)	Junio 2015
V1.1.2	Revisión periódica	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 e identificar la política de certificación correspondiente.

En concreto el identificador correspondiente a este tipo de certificados es:

1.3.6.1.4.1.17326.10.11.2

Índice de Contenido

1. Introducción *10*

1.1. Consideración Inicial **10**

1.2. Vista General **11**

1.3. Identificación **13**

1.4. Comunidad y Ámbito de Aplicación **13**

1.4.1 Autoridad de Certificación (AC) 13

1.4.2 Autoridad de Registro (AR) 13

1.4.3 Suscriptor 13

1.4.4 Tercero que confía 14

1.4.5 Solicitante 14

1.4.6 Ámbito de Aplicación y Usos 14

1.4.6.1 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 Solicitante. 16

2.1.3 Suscriptor 17

2.1.4 Tercero que confía. 17

2.1.5 Repositorio. 17

2.2. Responsabilidad **18**

2.2.1 Exoneración de responsabilidad 18

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones 18

2.3. Responsabilidad financiera **18**

2.4. Interpretación y ejecución **19**

2.4.1 Legislación 19

2.4.2 Independencia 19

2.4.3 Notificación 19

2.4.4 Procedimiento de resolución de disputas 19

2.5. Tarifas **19**

2.5.1 Tarifas de emisión de certificados y renovación 19

2.5.2 Tarifas de acceso a los certificados 19

2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados 20

2.5.4 Tarifas por el acceso al contenido de estas Políticas de Certificación 20

2.5.5 Política de reintegros 20

2.6. Publicación y repositorios **20**

2.6.1 Publicación de información de la AC 20

2.6.1.1 Políticas y Prácticas de Certificación 20

2.6.1.2 Términos y condiciones 20

2.6.1.3 Difusión de los certificados 21
2.6.2 Frecuencia de publicación 21
2.6.3 Controles de acceso 21

2.7. Auditorias 22
2.7.1 Frecuencia de las auditorias 22
2.7.2 Identificación y calificación del auditor 22
2.7.3 Relación entre el auditor y la AC 22
2.7.4 Tópicos cubiertos por la auditoria 22

2.8. Confidencialidad 22
2.8.1 Tipo de información a mantener confidencial 22
2.8.2 Tipo de información considerada no confidencial 23
2.8.3 Divulgación de información de revocación de certificados 23
2.8.4 Envío a la Autoridad Competente 23

2.9. Derechos de propiedad intelectual 23

3. Identificación y Autenticación 24

3.1. Registro inicial 24
3.1.1 Tipos de nombres 24
3.1.2 Pseudónimos 24
3.1.3 Reglas utilizadas para interpretar varios formatos de nombres 24
3.1.4 Unicidad de los nombres 24
3.1.5 Procedimiento de resolución de disputas de nombres 24
3.1.6 Reconocimiento, autenticación y función de las marcas registradas 25
3.1.7 Métodos de prueba de la posesión de la clave privada 25
3.1.8 Autenticación de la identidad de una organización 25

3.2. Renovación de la clave 25

3.3. Modificación de certificados 25

3.4. Reemisión después de una revocación 26

3.5. Solicitud de revocación 26

4. Requerimientos Operacionales 27

4.1. Solicitud de certificados 27

4.2. Petición de certificación cruzada 27

4.3. Emisión de certificados 27

4.4. Aceptación de certificados 28

4.5. Suspensión y revocación de certificados 28
4.5.1 Causas de revocación 28
4.5.2 Quién puede solicitar la revocación 29
4.5.3 Procedimiento de solicitud de revocación 29
4.5.4 Periodo de revocación 30
4.5.5 Suspensión 30
4.5.6 Procedimiento para la solicitud de suspensión 30
4.5.7 Límites del periodo de suspensión 30
4.5.8 Frecuencia de emisión de CRL's 30
4.5.9 Requisitos de comprobación de CRL's 30
4.5.10 Disponibilidad de comprobación on-line de la revocación 31

4.5.11 Requisitos de la comprobación on-line de la revocación 31
4.5.12 Otras formas de divulgación de información de revocación disponibles 31
4.5.13 Requisitos de comprobación para otras formas de divulgación de información de revocación 31
4.5.14 Requisitos especiales de revocación por compromiso de las claves 31

4.6. Procedimientos de Control de Seguridad 31
4.6.1 Tipos de eventos registrados 32
4.6.2 Frecuencia de procesado de Logs 33
4.6.3 Periodos de retención para los Logs de auditoría 33
4.6.4 Protección de los Logs de auditoría 34
4.6.5 Procedimientos de backup de los Logs de auditoría 34
4.6.6 Sistema de recogida de información de auditoria 34
4.6.7 Notificación al sujeto causa del evento 34
4.6.8 Análisis de vulnerabilidades 34

4.7. Archivo de registros 34
4.7.1 Tipo de archivos registrados 34
4.7.2 Periodo de retención para el archivo 35
4.7.3 Protección del archivo 35
4.7.4 Procedimientos de backup del archivo 35
4.7.5 Requerimientos para el sellado de tiempo de los registros 35
4.7.6 Sistema de recogida de información de auditoria 35
4.7.7 Procedimientos para obtener y verificar información archivada 35

4.8. Cambio de clave de la AC 36

4.9. Recuperación en caso de compromiso de la clave o desastre 36
4.9.1 La clave de la AC se compromete 36
4.9.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre 36

4.10. Cese de la AC 37

5. Controles de Seguridad Física, Procedimental y de Personal 38

5.1. Controles de Seguridad física 38
5.1.1 Ubicación y construcción 39
5.1.2 Acceso físico 39
5.1.3 Alimentación eléctrica y aire acondicionado 39
5.1.4 Exposición al agua 39
5.1.5 Protección y prevención de incendios 39
5.1.6 Sistema de almacenamiento. 39
5.1.7 Eliminación de residuos 39
5.1.8 Backup remoto 40

5.2. Controles procedimentales 40
5.2.1 Roles de confianza 40
5.2.2 Numero de personas requeridas por tarea 40
5.2.3 Identificación y autentificación para cada rol 41

5.3. Controles de seguridad de personal 41
5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación 41
5.3.2 Procedimientos de comprobación de antecedentes 42
5.3.3 Requerimientos de formación 42

5.3.4 Requerimientos y frecuencia de la actualización de la formación 42
5.3.5 Frecuencia y secuencia de rotación de tareas 42
5.3.6 Sanciones por acciones no autorizadas 42
5.3.7 Requerimientos de contratación de personal 43
5.3.8 Documentación proporcionada al personal 43

6. Controles de Seguridad Técnica 44

6.1. Generación e instalación del par de claves 44
6.1.1 Generación del par de claves de la AC 44
6.1.2 Generación del par de claves del suscriptor 44
6.1.3 Entrega de la clave privada al suscriptor 44
6.1.4 Entrega del CSR 44
6.1.5 Entrega de la clave pública de la CA a los Usuarios 44
6.1.6 Tamaño y periodo de validez de las claves del emisor 45
6.1.7 Tamaño y periodo de validez de las claves del suscriptor 45
6.1.8 Parámetros de generación de la clave pública 45
6.1.9 Comprobación de la calidad de los parámetros 45
6.1.10 Hardware / software de generación de claves 45
6.1.11 Fines del uso de la clave 46

6.2. Protección de la clave privada 46

6.3. Estándares para los módulos criptográficos 46
6.3.1 Control multipersona (n de entre m) de la clave privada 47
6.3.2 Depósito de la clave privada (key escrow) 47
6.3.3 Copia de seguridad de la clave privada 47
6.3.4 Archivo de la clave privada 47
6.3.5 Introducción de la clave privada en el módulo criptográfico 47
6.3.6 Método de activación de la clave privada 47
6.3.7 Método de desactivación de la clave privada 47
6.3.8 Método de destrucción de la clave privada 48

6.4. Otros aspectos de la gestión del par de claves 48
6.4.1 Archivo de la clave pública 48
6.4.2 Periodo de uso para las claves públicas y privadas 48

6.5. Datos de activación 48
6.5.1 Generación y activación de los datos de activación 48
6.5.2 Protección de los datos de activación 48
6.5.3 Otros aspectos de los datos de activación 48

6.6. Ciclo de vida del dispositivo seguro de creación de firma (DSCF) 48

6.7. Controles de seguridad informática 49
6.7.1 Requerimientos técnicos de seguridad informática específicos 49
6.7.2 Valoración de la seguridad informática 49

6.8. Controles de seguridad del ciclo de vida 50
6.8.1 Controles de desarrollo del sistema 50
6.8.2 Controles de gestión de la seguridad 50
6.8.2.1 Gestión de seguridad 50
6.8.2.2 Clasificación y gestión de información y bienes 50
6.8.2.3 Operaciones de gestión 51
6.8.2.4 Gestión del sistema de acceso 51

6.8.2.5 Gestión del ciclo de vida del hardware criptográfico 52
6.8.3 Evaluación de la seguridad del ciclo de vida 53

6.9. Controles de seguridad de la red 53

6.10. Controles de ingeniería de los módulos criptográficos 53

7. Perfiles de Certificado y CRL 54

7.1. Perfil de Certificado 54
7.1.1 Número de versión 54
7.1.2 Extensiones del certificado 54
7.1.3 Extensión con las facultades de representación especial. 54
7.1.4 Extensiones específicas 54
7.1.5 Identificadores de objeto (OID) de los algoritmos 54
7.1.6 Formato de nombres 55
7.1.7 Restricciones de los nombres 55

7.2. Perfil de CRL 55
7.2.1 Número de versión 55
7.2.2 CRL y extensiones 55

7.3. OCSP Profile 55
7.3.1 Número de versión 55
7.3.2 Extensiones OCSP 55

8. Especificación de la Administración 56

8.1. Autoridad de las políticas 56

8.2. Procedimientos de especificación de cambios 56

8.3. Publicación y copia de la política 56

8.4. Procedimientos de aprobación de la CPS 56

Anexo I. Acrónimos 57

Anexo II. Definiciones 59

1. Introducción

1.1. Consideración Inicial

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

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

La Declaración de Practicas de Certificación es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Suscriptor o Tercero 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 Practicas 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 "**que"** requerimientos de seguridad son necesarios para la emisión de los certificados. La CPS nos dice "**como**" 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 Camerfirma Express Corporate Server, y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF.

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

Esta política define las reglas y responsabilidades que debe seguir la Autoridad de Certificación de segundo nivel para la emisión de certificados de servidor seguro, imponiendo además ciertas obligaciones que deben ser tenidas en cuenta por los suscriptores y tercero que confía en virtud de su especial relación con este tipo de certificados.

El certificado de Servidor Seguro es necesario para ofrecer una garantía razonable al usuario de un navegador Internet que el sitio Web al que accede y cuya dirección se incorpora como titular del certificado digital, esta controlado por la entidad cuyo nombre también esta incorporado en el certificado digital. Adicionalmente el certificado permite garantizar la confidencialidad de los datos enviados y recibidos desde o a dicho sitio WEB mediante técnicas de encriptación.

- ✓ Los certificados emitidos bajo esta política requerirán la autenticación de la identidad y propiedad de una dirección en Internet.
- ✓ La AC revocará sus certificados según lo dispuesto en esta política.
- ✓ La AC deberá conservar los registros e incidencias de acuerdo con lo que se establece en esta política.
- ✓ Las funciones críticas del servicio deberán ser realizadas al menos por dos personas.
- ✓ La información personal recabada del suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación, el cual podrá ejercitar en todo caso sus oportunos derechos de información, rectificación y cancelación. La AC deberá respetar así mismo la normativa aplicable en materia de protección de datos.
- ✓ La actividad de la AC podrá ser sometida a la inspección de la Autoridad de la Políticas (PA) o por personal delegado por la misma.
- ✓ En lo que se refiere al contenido de esta Política de Certificación, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se

informe a este respecto. En la página web de Camerfirma (www.camerfirma.com) hay algunas informaciones útiles.

1.3. Identificación

Nombre de la Política:	Camerfirma Express Corporate Server
Descripción:	Acredita la propiedad del dominio en Internet y la confidencialidad de los datos trasmitidos desde el navegador del usuario y el sitio Web.
Versión:	1.1.1
Fecha de Emisión:	Junio 2015
Referencia (OID):	1.3.6.1.4.1.17326.10.11.2
Localización:	https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

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 Suscriptor y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una entidad (Suscriptor), a través de la emisión de un Certificado.

1.4.2 Autoridad de Registro (AR)

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

1.4.3 Suscriptor

Bajo esta Política, el Suscriptor es una entidad, la cual dispone de un Certificado Camerfirma Express Corporate Server.

A efectos de las presentes políticas de Certificación nos referiremos a una Entidad como aquella empresa u organización de cualquier tipo la cual tiene registrado un determinado dominio.

En el supuesto de que el Suscriptor sea un empresario individual, este actúa en nombre propio pero en el ámbito de su actividad.

1.4.4 Tercero que confía

En esta Política se entiende por Tercero que confía la persona que voluntariamente confía en el Camerfirma Express Corporate Server y se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

1.4.5 Solicitante

A los efectos de esta Política, se entenderá por Solicitante la persona física que solicita el Certificado Camerfirma Express Corporate Server.

1.4.6 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política se dirige tanto a entidades privadas, o públicas que poseen un dominio en Internet.

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

- Identificación de la Entidad que controla un sitio Web. Ofrece una garantía razonable al usuario de un aplicativo cliente de navegación en Internet (navegador) de que el sitio al que se accede es controlado por la entidad identificada en el certificado mediante su nombre, dirección fiscal e identificación fiscal.

- Permitir el intercambio de información de claves para establecer un canal de comunicación cifrado entre el navegador y el sitio Web.

- Asistir al usuario del navegador para asegurar la legitimidad de una entidad que declara gestionar un sitio Web, estableciendo un canal que sirva de ayuda para resolver problemas de direccionamientos relacionados con *phishing* y otras formas de fraude de identidad.

1.4.6.1 Usos Prohibidos y no Autorizados

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

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

La AC no se responsabilizará **EN NINGUN CASO** del contenido de las páginas Web bajo la URL identificada en el certificado.

1.5. Contacto

La Política de Certificación Camerfirma Express Corporate Server, 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.
5. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
6. Revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
7. Informar a los Suscriptores de la revocación de sus certificados, en tiempo y forma de acuerdo con la legislación Española vigente.
8. Publicar esta Política y las Prácticas correspondientes en su página web
9. Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los Suscriptores.
10. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
11. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

2.1.2 Solicitante.

El solicitante de un Certificado Camerfirma Express Corporate Server estará obligado a cumplir con lo dispuesto en estas políticas, por la normativa vigente y además a:

1. Suministrar a la AC la información necesaria para realizar una correcta identificación.

2. Realizar el pago del certificado conforme a la forma y medios establecidos por la AC.

3. Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.

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

2.1.3 Suscriptor

El Suscriptor de un Certificado Camerfirma Express Corporate Server estará obligado a cumplir con lo dispuesto en estas políticas, 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. Informar de la existencia de alguna causa de revocación.

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

2.1.4 Tercero que confía.

Será obligación de los Terceros que confían en un Certificado Camerfirma Express Corporate Server, a cumplir con lo dispuesto en estas políticas por la normativa vigente y además a:

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.

2.1.5 Repositorio.

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

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

2.2. Responsabilidad

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

1. La exactitud de toda la información contenida en el certificado en la fecha de su emisión
2. La garantía de que la clave pública y privada funcionan conjunta y complementariamente
3. La correspondencia entre el certificado solicitado y el certificado entregado
4. Cualquier responsabilidad que se establezca por la legislación vigente.

2.2.1 Exoneración de responsabilidad

La AC no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

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

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

La AC no se responsabilizará por las pérdidas por transacciones.

2.3. Responsabilidad financiera

La AC no asume ningún tipo de responsabilidad financiera.

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

2.4. Interpretación y ejecución

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación española vigente.

2.4.2 Independencia

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

2.4.3 Notificación

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

2.4.4 Procedimiento de resolución de disputas

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

2.5. Tarifas

2.5.1 Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los Terceros que confían en la página Web de Camerfirma.

2.5.2 Tarifas de acceso a los certificados

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

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

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

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

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

2.5.5 Política de reintegros

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

2.6. Publicación y repositorios

2.6.1 Publicación de información de la AC

2.6.1.1 Políticas y Prácticas de Certificación

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

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

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

2.6.1.2 Términos y condiciones

La AC pondrá a disposición de los Suscriptores y Terceros que confían los términos y condiciones del servicio. En concreto:

a) La AC pondrá a disposición de los Suscriptores y Terceros que confían los términos y condiciones relativos al uso de los certificados;

- Las limitaciones de uso.
- La información sobre cómo validar los certificados, incluyendo los requisitos para comprobar si un certificado ha sido revocado.
- Los límites de responsabilidad.
- El periodo de tiempo en que la información registrada será almacenada.

- Los procedimientos para la resolución de disputas.
- El ordenamiento jurídico aplicable.
- Si la AC ha sido acreditada conforme a la Política identificada en el certificado.

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

2.6.1.3 Difusión de los certificados

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

En concreto:

a) El certificado de la AC es público y se encontrará disponible en la página Web de Camerfirma.

b) El resto de los certificados estarán disponibles al público en la página Web de Camerfirma sólo en los casos en que el Suscriptor haya otorgado su consentimiento

c) La AC pondrá a disposición de los Terceros que confían los términos y condiciones referentes al uso de los certificados

d) La información a la que se refiere el punto a) estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la AC, la AC hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

2.6.2 Frecuencia de publicación

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

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

2.6.3 Controles de acceso

El acceso a la información será gratuito y estará a disposición de los suscriptores y Terceros que confían.

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

2.7. Auditorias

2.7.1 Frecuencia de las auditorias

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

2.7.2 Identificación y calificación del auditor

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

2.7.3 Relación entre el auditor y la AC

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

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

2.7.4 Tópicos cubiertos por la 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.

2.8. Confidencialidad

2.8.1 Tipo de información a mantener confidencial

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

2.8.2 Tipo de información considerada no confidencial

Se considerará como información no confidencial:

a) La contenida en la presente Política y en las Prácticas de Certificación

b) La información contenida en los certificados.

c) Cualquier información cuya publicidad sea impuesta normativamente

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

2.8.3 Divulgación de información de revocación de certificados

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

2.8.4 Envío a la Autoridad Competente

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

2.9. Derechos de propiedad intelectual

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

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Tipos de nombres

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

3.1.2 Pseudónimos

No se admitirán pseudónimos.

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 ACRONIMO que identifique a la empresa a la que está vinculada el titular del certificado. Esta alternativa es importante cuando un titular posee más de un certificado debido a su vinculación a más de una empresa. Algunos aplicativos solo muestran el nombre del titular a la hora de elegir un certificado del almacén para realizar un proceso de autenticación o firma. En estos casos el titular no tiene una forma rápida de diferenciar el certificado a usar.

El formato del CN dentro del certificado será:

"Nombre del Titular [ACRONIMO]"

3.1.4 Unicidad de los nombres

La AC se asegurará de que no existan dos certificados activos emitidos para la misma URL con información diferente.

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 de la entidad u otro elemento de identificación inequívoco, como el número de identificación fiscal.

3.1.7 Métodos de prueba de la posesión de la clave privada

El procedimiento usado por el suscriptor para la petición a la CA de la emisión del certificado, es la entrega de un fichero en formato PKCS#10 o CSR. Este fichero incorpora la clave pública generada en el servidor de páginas donde finalmente se instalara el certificado. Este fichero firmado con a clave privada es la prueba de posesión de esta.

3.1.8 Autenticación de la identidad de una organización

Los Certificados emitidos bajo la presente Política identifican a una entidad a cuyo nombre ha sido registrado un dominio. La RA utilizara los medios oportunos para asegurarse de la existencia de la organización. Entre estos medios se cuentan bases registrales externas. El identificativo fiscal de la organización se incorporara en el contenido del certificado.

3.2. Renovación de la clave

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

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

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

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

3.3. Modificación de certificados

Ante cualquier necesidad de modificación de certificados, la AC realizará una revocación del certificado y una nueva emisión con los datos corregidos.

3.4. Reemisión después de una revocación

La AC no realizará reemisiones.

3.5. Solicitud de revocación

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

4. Requerimientos Operacionales

4.1. Solicitud de certificados

Registro

a) Antes de comenzar el procedimiento de emisión, la AC deberá informar al suscriptor de los términos y condiciones relativos al uso del certificado

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

c) El proveedor de servicios deberá comprobar, la existencia de la entidad, del solicitante, de la existencia del dominio y la pertenencia de este a la entidad.

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

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

4.2. Petición de certificación cruzada

La AC identificará los procesos necesarios para realizar certificación cruzada.

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

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

4.3. Emisión de certificados

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

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

- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados

con el suscriptor o entre distintos componentes del sistema de certificación.

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

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

4.4. Aceptación de certificados

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

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

4.5. Suspensión y revocación de certificados

4.5.1 Causas de revocación

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

- Solicitud voluntaria del Suscriptor.

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

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

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

- Que se detecte que las claves privadas del Suscriptor o de la AC han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.

- Por incumplimiento por parte de la AC o el Suscriptor de las obligaciones establecidas en esta política.

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

- Por resolución judicial o administrativa que lo ordene.

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

4.5.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse únicamente por el suscriptor, un representante de la entidad a la que pertenece o por la propia AC.

Todas las solicitudes deberán ser en todo caso autenticadas.

4.5.3 Procedimiento de solicitud de revocación

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

La información relativa al retraso máximo entre la recepción de una petición de revocación y su paso al estado de revocado estará disponible para todos los usuarios. Este deberá ser como máximo de dos semanas.

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

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

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

La información relativa al estado de la revocación estará disponible las 24 del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no

esté bajo el control de la AC, la AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

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

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

4.5.4 Periodo de revocación

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

4.5.5 Suspensión

No se realiza suspensión

4.5.6 Procedimiento para la solicitud de suspensión

No aplicable

4.5.7 Límites del periodo de suspensión

No aplicable

4.5.8 Frecuencia de emisión de CRL's

La AC proporcionará la información relativa a la revocación de los certificados a través de una CRL 24h después de la última emisión o cada vez que se produzca una revocación y tendrá una validez de 48 horas.

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.

4.5.9 Requisitos de comprobación de CRL's

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

4.5.10 Disponibilidad de comprobación on-line de la revocación

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

4.5.11 Requisitos de la comprobación on-line de la revocación

El tercero que confía 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/Suscriptores, por lo que para la obtención del estado de un certificado deberán conocerse algunos parámetros del mismo como el e-mail.

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

4.5.12 Otras formas de divulgación de información de revocación disponibles

No estipulado.

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

No estipulado

4.5.14 Requisitos especiales de revocación por compromiso de las claves

No estipulado

4.6. Procedimientos de Control de Seguridad

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

General

a) Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la confidencialidad y la integridad de los registros relativos a los certificados, tanto de los actuales como de aquellos que hayan sido previamente almacenados.

b) Los registros relativos a los certificados deberán ser almacenados completa y confidencialmente de acuerdo con las prácticas de negocio.

c) Los registros relativos a los certificados deberán estar disponibles si estos son requeridos a efectos probatorios en los procedimientos legales.

d) El momento exacto en que se produjeron los eventos relativos a la gestión de los certificados deberá ser almacenado.

e) Los registros relativos a los certificados serán mantenidos durante un periodo de tiempo necesario para dotar de la evidencia legal necesaria a las firmas electrónicas.

f) Los eventos se registrarán de manera que no puedan ser fácilmente borrados o destruidos (excepto para su transferencia a medios duraderos) durante el periodo de tiempo en el que deban ser conservados

g) Los eventos específicos y la fecha de registro serán documentados por la AC

Registro

h) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que todos los eventos relativos al registro, incluyendo las peticiones de renovación y revocación serán registrados.

i) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada

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

Generación del certificado

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

l) La AC registrará todos los eventos relativos al ciclo de vida de los certificados

Gestión de la revocación

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

4.6.1 Tipos de eventos registrados

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

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

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

4.6.2 Frecuencia de procesado de Logs

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

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

4.6.3 Periodos de retención para los Logs de auditoría

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

4.6.4 Protección de los Logs de auditoría

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

4.6.5 Procedimientos de backup de los Logs de auditoría

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

4.6.6 Sistema de recogida de información de 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 auditoria
- todos los datos relativos a los certificados.
- solicitudes de emisión y revocación de certificados
- todos los certificados emitidos o publicados
- CRLs emitidas o registros del estado de los certificados generados

- la documentación requerida por los auditores
- 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

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

4.7.3 Protección del archivo

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

4.7.4 Procedimientos de backup del archivo

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

4.7.5 Requerimientos para el sellado de tiempo de los registros

No estipulado

4.7.6 Sistema de recogida de información de auditoria

No estipulado

4.7.7 Procedimientos para obtener y verificar información archivada

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

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

4.8. Cambio de clave de la AC

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

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 suscriptores, Terceros que confían 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 reestablecimiento.

4.10. Cese de la AC

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

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

- Informar a todos los suscriptores, Terceros que confían y otras ACs con los cuales tenga acuerdos u otro tipo de relación del cese.
- La AC revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- La AC realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y Terceros que confían.
- Las claves privadas de la AC serán destruidas o deshabilitadas para su uso.

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

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

- informar a las entidades afectadas
- transferencia de las obligaciones de la AC a otras partes
- cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aún no ha expirado.

En particular, la AC deberá:

- Informar puntualmente a todos los suscriptores, empleados y Terceros que confían con una anticipación mínima de 6 meses antes del cese
- Transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación

5. Controles de Seguridad Física, Procedimental y de Personal

5.1. Controles de Seguridad física

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

AC General

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

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

- Se establecerán controles para evitar el compromiso o robo de información

Emisión de certificados y gestión de revocaciones.

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

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

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

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

5.1.1 Ubicación y construcción

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

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

5.1.2 Acceso físico

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

5.1.3 Alimentación eléctrica y aire acondicionado

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

5.1.4 Exposición al agua

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

5.1.5 Protección y prevención de incendios

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

5.1.6 Sistema de almacenamiento.

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

5.1.7 Eliminación de residuos

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

5.1.8 Backup remoto

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

5.2. Controles procedimentales

5.2.1 Roles de confianza

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

Los roles de confianza incluyen las siguientes responsabilidades:

- **Responsable de seguridad:** asume la responsabilidad por la implementación de las políticas de seguridad así como gestión y revisión de logs.
- **Administradores de sistema:** Están autorizados para instalar, configurar y mantener de los sistemas y aplicaciones de confianza de la AC que soportan las operaciones de Certificación
- **Operador de sistema:** Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación
- **Administrador de CA:** Responsable de la Administración y control de gestión de los sistemas de confianza de la AC.
- **Operador de CA:** Realizan funciones de apoyo en el control dual de las operaciones de la CA.
- **Auditor de CA:** Realiza las labores de supervisión y control de la implementación de las políticas de seguridad

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

La separación de los roles de confianza serán detallados en la CPS

5.2.2 Numero 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

- La AC empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.
- Los roles de seguridad y responsabilidades especificadas en la política de seguridad de la AC, serán documentadas en la descripción del trabajo.
- Se deberá describir el trabajo del personal de la AC (temporal y fijo) desde el punto de vista de realizar un 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.
- El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados y gestión de revocaciones

e) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.

f) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la AC

g) El personal de la AC será formalmente designado para desempeñar roles de confianza por el responsable de seguridad

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

5.3.2 Procedimientos de comprobación de antecedentes

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

5.3.3 Requerimientos de formación

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

- Los principales mecanismos de seguridad de AC y/o AR
- Todo el software de PKI y sus versiones empleados en el sistema de la AC
- Todas las tareas de PKI que se espera que realicen
- Los procedimientos de resolución de contingencias y continuidad de negocio

5.3.4 Requerimientos y frecuencia de la actualización de la formación

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

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado

5.3.6 Sanciones por acciones no autorizadas

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

5.3.7 Requerimientos de contratación de personal

Ver el apartado 5.3.1 de este documento.

5.3.8 Documentación proporcionada al personal

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

6. Controles de Seguridad Técnica

6.1. Generación e instalación del par de claves

6.1.1 Generación del par de claves de la AC

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

En particular:

a) La generación de la clave de la AC se realizará en un entorno securizado físicamente por el personal adecuado según los roles de confianza y, al menos con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS

b) La generación de la clave de la AC se realizará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-2, en su nivel 3 o superior.

6.1.2 Generación del par de claves del suscriptor

El par de claves será generado por el suscriptor en el entorno del servidor que establecerá las comunicaciones SSL/TLS.

6.1.3 Entrega de la clave privada al suscriptor

La CA no gestionara claves privadas en este tipo de certificados.

6.1.4 Entrega del CSR

El suscriptor puede enviar el CSR al prestador bien mediante formulario de petición o bien mediante email.

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

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

a) La clave pública de la AC estará disponible a los usuarios 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 los usuarios a través de su página Web en al menos dos algoritmos resumen de uso común en el momento de realizarse.

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 **30 años**, después del cual deberán cambiarse estas claves.

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

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

6.1.7 Tamaño y periodo de validez de las claves del suscriptor

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

El periodo de uso de la clave pública y privada del suscriptor no excederá del periodo durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

6.1.8 Parámetros de generación de la clave pública

No estipulado

6.1.9 Comprobación de la calidad de los parámetros

No estipulado

6.1.10 Hardware / software de generación de claves

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

6.1.11 Fines del uso de la clave

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

La clave privada del Firmante/Suscriptor 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. Estas acciones deben quedar descritas en detalle en la DPC correspondiente. 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.

e) Establecer de un procedimiento de desactivación de la clave privada.

6.3. Estándares para los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 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.

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.

Al permitirse el uso de las claves para cifrado y no estar sujeto este certificado a los requerimientos de la ley de firma electrónica, las copias de las claves privadas de los suscriptores podrán ser custodiadas por el prestador. El prestador almacenara las claves de forma segura y establecerá un mecanismo seguro de entrega de la copia al titular cuando este la requiera.

6.3.4 Archivo de la clave privada

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

Las claves privadas del suscriptor pueden ser archivadas

6.3.5 Introducción de la clave privada en el módulo criptográfico

Ya visto

6.3.6 Método de activación de la clave privada

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

No aplicable a la clave privada del suscriptor

6.3.7 Método de desactivación de la clave privada

No aplicable

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.

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 creación de firma (DSCF)

No aplicable

6.7. Controles de seguridad informática

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

- identificación de todos los usuarios
- controles de acceso basados en privilegios
- control dual para ciertas operaciones relativas a la seguridad
- generación de logs, revisión de 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 suscriptor 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 previamente.

d) Los controles de seguridad y procedimientos operativos para las instalaciones de la AC, sistemas e información necesarios para los servicios de certificación serán documentados, implementados y mantenidos.

e) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se mantendrá la seguridad de información cuando la responsabilidad respecto a funciones de la AC haya sido subcontratada a otra organización

6.8.2.2 Clasificación y gestión de información y bienes

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

6.8.2.3 Operaciones de gestión

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

a) se protegerá la integridad de los sistemas de AC y de su información contra virus y software malintencionado o no autorizado

b) los daños derivados de incidentes de seguridad y los errores de funcionamiento deberán ser minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.

c) Los soportes serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados

d) Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de certificación.

Tratamiento de los soportes y seguridad

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

Planning del sistema

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

Reportes de incidencias y respuesta

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

Procedimientos operacionales y responsabilidades

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

6.8.2.4 Gestión del sistema de acceso

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

AC General

a) Se implementarán controles (p. Ej. Cortafuegos) para proteger la red interna de redes externas accesibles por terceras partes.

b) Los datos sensibles serán protegidos cuando estos sean transmitidos por redes no protegidas.

c) La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de usuarios (incluyendo operadores, administradores y cualquier usuario que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de usuarios, auditorias 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

El acceso físico a los dispositivos debe protegerse mediante una adecuada gestión de red con una arquitectura que orden 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 debe realizar de forma cifrada mediante uso de protocolos correspondientes.

6.10. Controles de ingeniería de los módulos criptográficos

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

7. Perfiles de Certificado y CRL

7.1. Perfil de Certificado

Todos los certificados emitidos bajo esta política serán conformes al estándar X.509 versión 3 y al RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".

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 a la dirección de correo marcada en el punto 1.5.

7.1.3 Extensión con las facultades de representación especial.

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

7.1.4 Extensiones específicas

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

7.1.5 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será 1.2.840.113549.1.1.5

El identificador de objeto del algoritmo de la clave pública será rsaEncryption 1.2.840.113549.1.1.1

7.1.6 Formato de nombres

Se incluirá la información indicada en el apartado 7.1.5 del documento de la Declaración de Prácticas de Certificación.

7.1.7 Restricciones de los nombres

Se seguirán las restricciones establecidas en el apartado 7.1.6 del documento de la Declaración de Prácticas de Certificación.

7.2. Perfil de CRL

El perfil está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite a la dirección de correo marcada en el punto 1.5.

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 está redactado en un documento independiente. Dicho documento debe estar a disposición de cualquier tercero que lo solicite a la dirección de correo marcada en el punto 1.5.

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.

Cualquier comunicación de los terceros que confían afectados puede presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación en la dirección email descrita en el punto 1.5 de este documento.

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-1 *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 suscriptor.
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 si 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
Suscriptor	Dentro del contexto de las políticas de certificación de Camerfirma, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Tercero que confía	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 19:27:31
Certificado Digital