POLÍTICA DE CERTIFICACIÓN

Camerfirma

Certificado Digital

GLOBAL CHAMBERSIGN ROOT

Versión 1.0.1

Idioma: **Castellano**
Fecha: **23 de julio de 2003**
Estado del documento: **Activo**

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	PUBLICACIÓN
1.0.	Creación del documento	Julio 2003
1.0.1	Revisión	Agosto 2018

Índice de Contenido

1. Introducción 8

1.1. Vista General 8

1.2. Identificación 10

1.3. Comunidad y Ámbito de Aplicación 10

1.3.1 Root CA 10
1.3.2 Autoridad de Certificación delegada (AC delegada) 10
1.3.3 Autoridad de Registro (AR) 11
1.3.4 Suscriptor 11
1.3.5 Usuario 11
1.3.6 Solicitante 11
1.3.7 Ámbito de Aplicación y Usos 11
1.3.7.1 Usos Prohibidos y no Autorizados 12

1.4. Contacto 12

2. Cláusulas Generales 13

2.1. Obligaciones 13

2.1.1 Root CA 13
2.1.2 AC 13

2.2. Repositorio 14

2.3. Responsabilidad 15

2.3.1 Exoneración de responsabilidad 15
2.3.2 Límite de responsabilidad en caso de pérdidas por transacciones 16

2.4. Responsabilidad financiera 16

2.5. Interpretación y ejecución 16

2.5.1 Legislación 16
2.5.2 Independencia 16
2.5.3 Notificación 17
2.5.4 Procedimiento de resolución de disputas 17

2.6. Tarifas 17

2.6.1 Tarifas de acceso a los certificados 17
2.6.2 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados 17
2.6.3 Tarifas por el acceso al contenido de estas Políticas de Certificación 17

2.7. Publicación y repositorios 18

2.7.1 Publicación de información de la AC 18
2.7.1.1 Políticas y Prácticas de Certificación 18
2.7.1.2 Términos y condiciones 18
2.7.1.3 Difusión de los certificados 18
2.7.2 Frecuencia de publicación 18
2.7.3 Controles de acceso 19

2.8. Auditorias 19

2.8.1 Frecuencia de las auditorias 19
2.8.2 Identificación y calificación del auditor 19
2.8.3 Relación entre el auditor y la Root CA 19
2.8.4 Tópicos cubiertos por la auditoria 19
2.8.5 Auditoria en las AC's delegadas 20

2.9. Confidencialidad 20
2.9.1 Tipo de información a mantener confidencial 20
2.9.2 Tipo de información considerada no confidencial 20
2.9.3 Divulgación de información de revocación de certificados de CA 21
2.9.4 Envío a la Autoridad Competente 21

2.10. Derechos de propiedad intelectual 21

3. Identificación y Autenticación 22

3.1. Registro inicial 22
3.1.1 Tipos de nombres 22
3.1.2 Pseudónimos 22
3.1.3 Reglas utilizadas para interpretar varios formatos de nombres 22
3.1.4 Unicidad de los nombres 22
3.1.5 Procedimiento de resolución de disputas de nombres 22
3.1.6 Reconocimiento, autenticación y función de las marcas registradas 23
3.1.7 Métodos de prueba de la posesión de la clave privada 23
3.1.8 Autenticación de la identidad de una organización 23
3.1.9 Autenticación de la identidad de un individuo 23

3.2. Renovación de la clave 23

3.3. Reemisión después de una revocación 23

3.4. Solicitud de revocación 24

4. Requerimientos Operacionales 25

4.1. Solicitud de certificados 25

4.2. Petición de certificación cruzada 25

4.3. Emisión de certificados 26

4.4. Aceptación de certificados 26

4.5. Revocación de certificados 26
4.5.1 Causas de revocación 26
4.5.2 Quién puede solicitar la revocación 27
4.5.3 Procedimiento de solicitud de revocación 27
4.5.4 Periodo de revocación 28
4.5.5 Suspensión 28
4.5.6 Procedimiento para la solicitud de suspensión 28
4.5.7 Límites del periodo de suspensión 28
4.5.8 Frecuencia de emisión de ARL's 28
4.5.9 Requisitos de comprobación de ARL's 29
4.5.10 Disponibilidad de comprobación on-line de la revocación 29
4.5.11 Requisitos de la comprobación on-line de la revocación 29
4.5.12 Otras formas de divulgación de información de revocación disponibles 29
4.5.13 Requisitos de comprobación para otras formas de divulgación de Información de revocación 29

4.5.14 Requisitos especiales de revocación por compromiso de las claves 30

4.6. Procedimientos de Control de Seguridad 30
4.6.1 Tipos de eventos registrados 31
4.6.2 Frecuencia de procesado de Logs 32
4.6.3 Periodos de retención para los Logs de auditoria 32
4.6.4 Protección de los Logs de auditoría 33
4.6.5 Procedimientos de backup de los Logs de auditoría 33
4.6.6 Sistema de recogida de información de auditoria 33
4.6.7 Notificación al sujeto causa del evento 33
4.6.8 Análisis de vulnerabilidades 33

4.7. Archivo de registros 34
4.7.1 Tipo de archivos registrados 34
4.7.2 Periodo de retención para el archivo 34
4.7.3 Protección del archivo 34
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 35

4.9. Recuperación en caso de compromiso de la clave o desastre 36
4.9.1 La clave de la Root CA 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 Root CA 36

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. 40
5.1.7 Eliminación de residuos 40
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 41
5.2.3 Identificación y autentificación para cada rol 41

5.3. Controles de seguridad de personal 42
5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación 42
5.3.2 Procedimientos de comprobación de antecedentes 43
5.3.3 Requerimientos de formación 43
5.3.4 Requerimientos y frecuencia de la actualización de la formación 43
5.3.5 Frecuencia y secuencia de rotación de tareas 43
5.3.6 Sanciones por acciones no autorizadas 43

5.3.7 Requerimientos de contratación de personal 44
5.3.8 Documentación proporcionada al personal 44

6. Controles de Seguridad Técnica 45

6.1. Generación e instalación del par de claves 45
6.1.1 Generación del par de claves 45
6.1.2 Entrega de la clave pública de la Root CA a los Usuarios 45
6.1.3 Tamaño y periodo de validez de las claves del emisor 46
6.1.4 Parámetros de generación de la clave pública 46
6.1.5 Comprobación de la calidad de los parámetros 46
6.1.6 Hardware/software de generación de claves 46
6.1.7 Fines del uso de la clave 46

6.2. Protección de la clave privada 47

6.3. Estándares para los módulos criptográficos 47
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 48
6.3.4 Archivo de la clave privada 48
6.3.5 Introducción de la clave privada en el módulo criptográfico 48
6.3.6 Método de activación de la clave privada 48
6.3.7 Método de destrucción de la clave privada 48

6.4. Otros aspectos de la gestión del par de claves 49
6.4.1 Archivo de la clave pública 49
6.4.2 Periodo de uso para las claves públicas y privadas 49

6.5. Controles de seguridad informática 49
6.5.1 Requerimientos técnicos de seguridad informática específicos 49
6.5.2 Valoración de la seguridad informática 50

6.6. Controles de seguridad del ciclo de vida 50
6.6.1 Controles de desarrollo del sistema 50
6.6.2 Controles de gestión de la seguridad 50
6.6.2.1 Gestión de seguridad 50
6.6.2.2 Clasificación y gestión de información y bienes 51
6.6.2.3 Operaciones de gestión 51
6.6.2.4 Gestión del sistema de acceso 52
6.6.2.5 Gestión del ciclo de vida del hardware criptográfico 53
6.6.3 Evaluación de la seguridad del ciclo de vida 53

6.7. Controles de seguridad de la red 53

6.8. Controles de ingeniería de los módulos criptográficos 54

7. Perfiles de Certificado y CRL 55

7.1. Perfil de Certificado 55
7.1.1 Número de versión 55
7.1.2 Extensiones del certificado 55
7.1.3 Identificadores de objeto (OID) de los algoritmos 57
7.1.4 Restricciones de los nombres 57

7.2. Perfil de CRL 57
7.2.1 Número de versión 58

7.2.2 CRL y extensiones 58
8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN 59
8.1. Autoridad de las políticas 59
8.2. Procedimientos de especificación de cambios 59
8.3. Publicación y copia de la política 59
***8.4.* Procedimientos de aprobación de la CPS 60**
ANEXO I. ACRÓNIMOS 61
ANEXO II. DEFINICIONES 64

1. Introducción

1.1. Vista General

El presente documento especifica la Política de Certificación de la Global Chambersign Root y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF.

Esta política define las reglas y responsabilidades que debe seguir la Root CA y aquellas Autoridades de certificación, aprobadas por ésta, que deseen formar parte de la estructura de certificación Chambersign Global de Camerfirma.

De esta forma, cualquier AC que forme parte de la estructura de certificación de la Global Chambersign Root, deberá ajustarse a los niveles de seguridad que se detallan en esta política de certificación y deberán informar a sus suscriptores de su existencia.

Las AC's delegadas que emitan certificados de entidad final deberán cumplir además lo dispuesto en las respectivas políticas de certificación en virtud de los certificados que emitan

Los certificados emitidos bajo esta política requerirán la autenticación de la identidad de las AC's y la verificación de la adecuación de sus procedimientos a la presente política.

La CA Root revocará los certificados de las AC's delegadas según lo dispuesto en esta política.

La CA Root 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 actividad de las AC's delegadas podrán ser sometidas 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.

1.2. Identificación

Nombre de la Política:	Política de Certificación Global Chambersign Root
Descripción:	Define los criterios básicos a seguir por la Root CA y por las AC's que emitan certificados digitales bajo su jerarquía.
Versión:	1.0.1
Fecha de Emisión:	Julio de 2003
Referencia (OID):	1.3.6.1.4.1.17326.10.1.1
Localización:	https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

1.3. Comunidad y Ámbito de Aplicación

1.3.1 Root CA

Es la entidad encargada de autorizar y emitir los certificados de las Autoridades de Certificación.

1.3.2 Autoridad de Certificación delegada (AC delegada)

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, en las relaciones electrónicas, vinculando una determinada clave pública con una persona (Suscriptor) relacionada a una entidad concreta, a través de la emisión de un Certificado.

Pueden emitir Certificados bajo la jerarquía Chambersign Global de Camerfirma, las Autoridades de Certificación cuya Política o CPS esté en conformidad con esta Política de Certificación y hayan sido previamente autorizados.

1.3.3 Autoridad de Registro (AR)

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

1.3.4 Suscriptor

Bajo esta Política el Suscriptor es una persona física, vinculada a una determinada entidad, poseedor de un dispositivo de creación de firma con un Certificado Digital emitido por una AC autorizada por Camerfirma.

1.3.5 Usuario

En esta Política se entiende por Usuario la persona que voluntariamente confía en el Certificado emitido por una AC delegada, lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado y en consecuencia se sujeta a lo dispuesto en esta Política, por lo que no se requerirá acuerdo posterior alguno.

1.3.6 Solicitante

A los efectos de esta Política, se entenderá por Solicitante la persona física que solicita el Certificado emitido por un a AC delegada.

1.3.7 Ámbito de Aplicación y Usos

El Certificado emitido bajo la presente Política será empleado únicamente para la firma de certificados de AC's delegadas y firma de ARL's

1.3.7.1 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, en la CPS y en los contratos firmados con la Autoridad de Certificación.

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

1.4. Contacto

La Política de Certificación de Chambersign Global Root de Camerfirma, está administrada y gestionada por el Departamento Jurídico de Camerfirma, 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 Root CA

La Root CA está obligada a cumplir las siguientes obligaciones:

1. Respetar lo dispuesto en esta política

2. Proteger su información contra pérdidas, destrucciones y falsificaciones.

3. Respetar lo dispuesto por la legislación relativa a la protección de datos personales

4. Proteger sus claves privadas de forma segura

5. Emitir certificados a las CA's delegadas de forma segura

6. Revocar los certificados según lo dispuesto en esta política y publicar la correspondiente ARL.

7. Informar a las AC's delegadas de los cambios que se produzcan en las presentes políticas

2.1.2 AC

Las AC's delegadas 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 de entidad final conforme a esta Política y a los estándares de aplicación.

4. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos

5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente.

6. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

7. Revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL

8. Informar a los Suscriptores de la revocación o suspensión de sus certificados.

9. Publicar esta Política y las Prácticas correspondientes en su página web.

10. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia.

11. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante perdida o destrucción o falsificación

12. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

2.2. Repositorio

La información relativa a la publicación y revocación de los certificados se mantendrá accesible al público.

La Root CA 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.

2.3. Responsabilidad

La Root CA será responsable del daño causado ante la AC delegada 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 de la AC delegada en la fecha de su emisión.

2. la garantía de que, en el momento de la entrega del certificado, obra en poder de la AC delegada, la clave privada correspondiente a la clave pública dada o identificada en el certificado.

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

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

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

2.3.1 Exoneración de responsabilidad

La Root CA 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 ARL's emitidos por la Root CA.

4. Por el uso de la información contenida en el Certificado o en la ARL.

5. Por el incumplimiento de las obligaciones establecidas para la AC delegada, el Suscriptor o Usuarios en la normativa vigente, las Políticas de Certificación o en las CPS's.

6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.

7. Fraude en la documentación presentada por la AC delegada.

8. Cuando el usuario que confía en un certificado emitido por una AC de la jerarquía no compruebe la vigencia o aplicabilidad del certificado

2.3.2 Límite de responsabilidad en caso de pérdidas por transacciones

No aplicable.

2.4. Responsabilidad financiera

No aplicable.

2.5. Interpretación y ejecución

2.5.1 Legislación

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

2.5.2 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.

2.5.3 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.

2.5.4 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. Tanto las AC's que emitan certificados conforme a esta política, como suscriptores, signatarios, usuarios, terceros que confían o cualquier tercero con interés legítimo vendrán obligados, por la mera aceptación de esta política, a cumplir el laudo que se dicte en el marco del arbitraje.

2.6. Tarifas

2.6.1 Tarifas de acceso a los certificados

El acceso a los certificados de CA emitidos será gratuito.

2.6.2 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.

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

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

2.7. Publicación y repositorios

2.7.1 Publicación de información de la AC

2.7.1.1 Políticas y Prácticas de Certificación

La Root CA y las AC's delegadas estarán obligadas a publicar la información relativa a sus Políticas y Prácticas de Certificación.

La presente Política de Certificación será pública y debe ser accesible públicamente.

La CPS y las Políticas de Certificación concretas para cada tipo de certificado de entidad final serán así mismo públicas y se pondrán a disposición del público en la dirección de Internet del emisor.

2.7.1.2 Términos y condiciones

La Root CA pondrá a disposición de las AC's delegadas y Usuarios los términos y condiciones del servicio.

2.7.1.3 Difusión de los certificados

La Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para las AC's delegadas y Usuarios.

El certificado de la Root CA es público y se encontrará disponible en la página web del emisor. Esta información 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 Root CA, la Root CA hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

La comprobación de integridad del certificado de la Root CA podrá hacerse a través del notario autorizante del acta que recoge la ceremonia de generación de las claves. La información sobre el protocolo notarial que recoge el acto de generación y del MD5 y SHA1 podrá obtenerse a través de la web del emisor.

2.7.2 Frecuencia de publicación

La Root CA deberá publicar la información contenida en el repositorio una vez que tenga conocimiento de la existencia o modificación de la misma.

2.7.3 Controles de acceso

El acceso a la información anterior será gratuito y estará a disposición de las AC's delegadas y usuarios.

2.8. Auditorias

2.8.1 Frecuencia de las auditorias

La Root CA deberá realizar auditorías con una periodicidad mínima anual, salvo que se establezca un plazo menor por la normativa vigente.

2.8.2 Identificación y calificación del auditor

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

2.8.3 Relación entre el auditor y la Root CA

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

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

2.8.4 Tópicos cubiertos por la auditoria

La auditoria deberá verificar en todo caso:

a) Que la Root CA tiene un sistema que garantice la calidad del servicio prestado

b) Que la Root CA cumple con los requerimientos de esta Política de Certificación

c) Que la CPS y las Políticas concretas de la Root CA 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.

2.8.5 Auditoria en las AC's delegadas

Todas las AC's delegadas y las AR's empleadas por éstas, deben ser auditadas en las mismas condiciones que la Root CA.

2.9. Confidencialidad

2.9.1 Tipo de información a mantener confidencial

Se determinará por la Root CA la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la normativa vigente en materia de protección de datos.

2.9.2 Tipo de información considerada no confidencial

Se considerará como información no confidencial:

a) La contenida en la presente Política y en la CPS

b) La información contenida en los certificados de las AC's delegadas.

c) Cualquier información cuya publicidad sea impuesta normativamente

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

2.9.3 Divulgación de información de revocación de certificados de CA

La forma de difundir la información relativa a la suspensión o revocación de un certificado de AC delegada se realizará mediante la publicación de las correspondientes ARLs.

2.9.4 Envío a la Autoridad Competente

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

2.10. Derechos de propiedad intelectual

Camerfirma 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 AC Camerfirma SA sin la autorización expresa por su parte. No obstante, no necesitará autorización de AC Camerfirma SA 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

Todas las AC's delegadas requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

3.1.2 Pseudónimos

No serán admitidos pseudónimos para los certificados de AC's delegadas.

3.1.3 Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.4 Unicidad de los nombres

La Root CA deberá confirmar la unicidad de los nombres de los certificados de CA.

3.1.5 Procedimiento de resolución de disputas de nombres

Se atenderá a lo dispuesto en el apartado 2.5.4 de este documento, salvo que se pruebe fehacientemente su titularidad y sea pertinente a la función para la que se requiera el certificado, a juicio de los responsables de la AC que deba evaluarlo

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

No se admitirá la identificación en función de marcas registradas.

3.1.7 Métodos de prueba de la posesión de la clave privada

La Root CA deberá tomar las medidas necesarias que aseguren que la AC delegada está en posesión de la clave privada asociada a su clave pública.

3.1.8 Autenticación de la identidad de una organización

Ver 4.1

3.1.9 Autenticación de la identidad de un individuo

Ver 4.1

3.2. Renovación de la clave

La Root CA deberá comprobar que la información contenida en el certificado de CA es todavía válida.

La Root CA podrá emitir un nuevo certificado de CA usando la anterior clave pública de la AC delegada.

3.3. Reemisión después de una revocación

La Root CA no realizará reemisiones.

3.4. Solicitud de revocación

Todas las solicitudes de revocación deberán ser autenticadas y firmadas por al menos un representante de la AC delegada.

4. Requerimientos Operacionales

4.1. Solicitud de certificados

La AC se asegurara que las AC's delegadas están correctamente identificadas y autorizados y que la petición de generación del certificado de CA es completa.

Registro

a) Antes de comenzar una relación contractual, la Root CA deberá informar a la AC delegada de los términos y condiciones relativos a la prestación del servicio y el uso del certificado de CA.

b) La Root CA deberá comprobar, la identidad y los atributos específicos de la AC delegada. La comprobación de la identidad se realizará en todo caso mediante la personación física de al menos un representante de la AC delegada y la exhibición por éste de la información relativa a la existencia de la entidad y su propia vinculación con la entidad.

c) La AC delegada deberá facilitar su dirección física u otros datos que permitan contactar con sus representantes.

d) La Root CA deberá registrar toda la información usada para comprobar la identidad de la AC delegada.

e) La AC deberá guardar el contrato firmado con la AC delegada.

f) La Root CA deberá cumplir con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos.

4.2. Petición de certificación cruzada

La Root CA identificará los procesos necesarios para realizar certificación cruzada.

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

- La Root CA deberá confirmar la unicidad de los DN asignados a las AC's delegadas.
- La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con la AC delegada o entre distintos componentes del sistema de certificación.
- La emisión de los certificados y la generación de las claves de las AC's delegadas deberá hacerse de acuerdo a una ceremonia de creación de clave que garantice la seguridad de todo el procedimiento.

4.4. Aceptación de certificados

La entrega del certificado y la firma del contrato de adhesión al sistema de certificación implicarán la aceptación del certificado por parte de la AC delegada.

La aceptación del certificado deberá realizarse de forma expresa y por escrito. Podrá considerarse prueba válida de aceptación el pago de la tarifa que sea de aplicación.

.

4.5. Revocación de certificados

4.5.1 Causas de revocación

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

- Que se detecte que las claves privadas de la Root CA o la AC delegada 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 a la AC delegada.
- Cambios en el contenido del certificado de la AC delegada.
- Cese en la actividad de la AC delegada como prestador de servicios de

certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.

- Por la decisión unilateral de la AC delegada o la Root CA.
- Por incumplimiento por parte de la AC delegada de las obligaciones establecidas en esta política.
- Por la resolución del contrato con la AC delegada.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la extinción de la entidad.
- Por la concurrencia de cualquier otra causa especificada en la presente política.
- Por falta de pago o de cumplimiento de otras condiciones contractuales entre la Root CA y las AC's delegadas

4.5.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por la AC delegada, por la propia Root CA, o por terceros interesados de buena fe que puedan demostrar fehacientemente que se producen condiciones que exijan la revocación.

Todas las solicitudes deberán ser en todo caso autenticadas.

4.5.3 Procedimiento de solicitud de revocación

La AC delegada cuyo certificado se haya revocado deberá ser informada del cambio de estado de su certificado. La Root CA 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 ARL, en su caso, será firmada por la Root CA o por una autoridad de confianza de la Root CA.

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

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

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

4.5.4 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 existe suspensión de certificados de CA

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 ARL's

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

La AC actualizará y publicará la ARL dentro de las 48 horas siguientes a la recepción de una solicitud de revocación que haya sido previamente validada, y al menos con una frecuencia mensual si no se han producido cambios en la ARL.

4.5.9 Requisitos de comprobación de ARL's

Los usuarios deberán comprobar el estado de los certificados de las AC's delegada en los cuales va a confiar, debiendo comprobar en todo caso la última ARL emitida.

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 Root CA, ésta 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

No estipulado

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 Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a un certificado de CA 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 de CA, tanto de los actuales como de aquellos que hayan sido previamente almacenados.

b) Los registros relativos a los certificados de CA deberán ser almacenados completa y confidencialmente.

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

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

e) 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

f) Los eventos específicos y la fecha de registro serán documentados por la Root CA

Registro

g) La Root CA 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.

h) La Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada, incluyendo la siguiente:

- La documentación presentada por la AC delegada para el registro
- Método empleado para comprobar la validez de los documentos identificativos, si existe

Generación del certificado

i) La Root CA registrará todos los eventos relativos al ciclo de vida de sus propias claves.

j) La Root CA registrará todos los eventos relativos al ciclo de vida de los certificados

de CA.

Gestión de la revocación

k) La Root CA 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 Root CA. Estos incluirán eventos como:

- encendido y apagado del sistema
- encendido y apagado de la aplicación de la Root CA
- intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- cambios en los detalles de la Root CA 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 Root CA a través de la red.
- intentos de accesos no autorizados al sistema de archivos
- generación de claves propias
- creación y revocación de certificados de CA

- intentos de dar de alta, eliminar, habilitar, deshabilitar y actualizar AC's delegadas

- acceso físico a los logs

- cambios en la configuración y mantenimiento del sistema

- cambios personales

- registros de la destrucción de los medios que contienen las claves, datos de activación

4.6.2 Frecuencia de procesado de Logs

La Root 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 Root 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 auditoria

La información almacenada deberá ser conservada durante el tiempo marcado por la legislación vigente o por las normas técnicas aplicables.

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 Root CA o por delegación de esta.

- todos los datos de la auditoría del sistema.
- todos los datos relativos a los certificados.
- solicitudes de emisión y revocación de certificados de CA.
- todos los certificados de AC's delegadas emitidos o publicados.
- ARL's emitidas o registros del estado de los certificados generados.
- historial de claves generadas.
- las comunicaciones entre los elementos de la PKI.

La Root CA es responsable del correcto archivo de todo este material

4.7.2 Periodo de retención para el archivo

La información archivada 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 Root CA 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 Root CA caduque se deberá realizar un cambio de claves. La vieja CA y su clave privada se desactivaran y se generara 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 publica 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 Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar en caso de desastre o compromiso de su clave privada que éstas serán restablecidas tan pronto como sea posible.

4.9.1 La clave de la Root CA se compromete

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

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

- Informar a todos los usuarios y a las AC's delegadas 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 Root CA debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

La Root CA debe reestablecer los servicios de acuerdo con esta política dentro de las 48 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 Root CA

La Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a las AC's delegadas o usuarios 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 usuarios y AC's delegadas del cese.

- La Root CA revocará toda autorización para actuar en su nombre en el procedimiento de emisión de certificados.

- La Root CA 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 usuarios.

- Las claves privadas de la Root CA serán destruidas o deshabilitadas para su uso.

b) 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 Root CA a otras partes

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

En particular, la Root CA deberá:

- informar puntualmente a todas las AC's delegadas y usuarios 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.

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:

General

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

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

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

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

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

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

f) Los controles de seguridad física y ambiental 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 ambiental de la Root CA 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 y protección antirrobo.

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

5.1.1 Ubicación y construcción

Las instalaciones de la Root CA 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 Root CA 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 certificación.

5.1.4 Exposición al agua

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

5.1.5 Protección y prevención de incendios

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

5.1.6 Sistema de almacenamiento.

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

5.1.7 Eliminación de residuos

La Root CA 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 serán destruidos, así como que la información que contengan será irrecuperable.

5.1.8 Backup remoto

La Root CA 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 Root CA, 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. Adicionalmente, aprobará la generación / revocación de certificados de CA.

- Administradores de sistema: están autorizados para instalar, configurar y mantener los sistemas de confianza de la Root CA para la generación del certificado y gestión de la revocación.

- Operadores de sistema: responsable por el buen funcionamiento diario de los sistemas de confianza de la Root CA. Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación.

- Auditores del sistema: están autorizados para ver y mantener los archivos y los logs de los sistemas de confianza de la Root CA.

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

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

5.2.2 Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

- La generación, reconstrucción y activación de la clave privada de la Root CA.

- La recuperación y back-up de la clave privada de la Root CA.

- La emisión de certificados de las AC's delegadas.

- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la Root CA.

5.2.3 Identificación y autentificación para cada rol

La Root CA 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 Root CA 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:

General

a) La Root CA empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.

b) Los roles de seguridad y responsabilidades especificadas en la política de seguridad de la Root CA, serán documentados en la descripción del trabajo.

c) Se deberá describir el trabajo del personal de la Root CA (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 especificas.

d) El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados de CA y gestión de revocaciones

e) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de PKI 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 Root CA.

g) El personal de la Root CA 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 Root CA 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 Root CA 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 Root CA debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de PKI, recibirá una formación relativa a:

- Los principales mecanismos de seguridad de la Root CA
- 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 Root CA deberá fijar las posibles sanciones por la realización de acciones no autorizadas.

5.3.7 Requerimientos de contratación de personal

Ya descrito en el apartado 5.3.1.

5.3.8 Documentación proporcionada al personal

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

6. Controles de Seguridad Técnica

6.1. Generación e instalación del par de claves

6.1.1 Generación del par de claves

La Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus propias claves y las de las AC's delegadas sean generadas de acuerdo a los estándares.

En particular:

a) La generación de la clave de la Root CA 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 Root CA 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 Entrega de la clave pública de la Root CA a los Usuarios

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

a) La clave pública de la Root CA 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 Root CA y su fingerprint (huella digital) estarán a disposición de los usuarios a través de su página web.

6.1.3 Tamaño y periodo de validez de las claves del emisor

La Root CA deberá usar claves basadas en el algoritmo RSA con una longitud descrita en las prácticas de certificación y que garanticen la seguridad criptográfica según el estado del arte.

El periodo de uso de una clave privada será como máximo de 25 años para la Root CA y de 10 años para las AC's delegadas.

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

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

6.1.4 Parámetros de generación de la clave pública

No estipulado

6.1.5 Comprobación de la calidad de los parámetros

No estipulado

6.1.6 Hardware/software de generación de claves

Las claves de la Root CA y de las CA's delegadas deberán ser generadas en un módulo criptográfico validado al menos por el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente

6.1.7 Fines del uso de la clave

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

6.2. *Protección de la clave privada*

La Root CA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus claves privadas continúan siendo confidenciales y mantienen su integridad. En particular:

a) La clave privada 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 Root CA esté fuera del módulo criptográfico esta deberá estar cifrada

c) Se deberá hacer un back up de la clave privada de firma, 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 se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

6.3. *Estándares para los módulos criptográficos*

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

6.3.1 Control multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona para la reconstrucción y activación de la clave privada de la Root 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 Root CA 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 Root CA deberá realizar una copia de back up en un centro externo 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.

6.3.4 Archivo de la clave privada

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

6.3.5 Introducción de la clave privada en el módulo criptográfico

Ya estipulado

6.3.6 Método de activación de la clave privada

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

6.3.7 Método de destrucción de la clave privada

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

Todas las copias de la clave privada de firma de la Root CA deberá ser destruidas de forma que la clave privada no pueda ser recuperada

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

6.4. Otros aspectos de la gestión del par de claves

6.4.1 Archivo de la clave pública

La Root CA deberá conservar todas las claves públicas de verificación

6.4.2 Periodo de uso para las claves públicas y privadas

Ya visto.

6.5. Controles de seguridad informática

La Root CA 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

6.5.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de la Root CA incluirá las siguientes funcionalidades:

- control de acceso a los servicios de CA 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 de los datos de auditoriaauditoria de eventos relativos a la seguridad
- auto-diagnóstico de seguridad relacionado con los servicios de la Root CA

- Mecanismos de recuperación de claves y del sistema de Root CA

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

6.5.2 Valoración de la seguridad informática

No estipulado

6.6. Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo del sistema

La Root CA empleará sistemas fiables y productos que estén protegidos contra modificaciones.

6.6.2 Controles de gestión de la seguridad

6.6.2.1 Gestión de seguridad

La Root CA 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 Root CA 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 Root CA en los acuerdos concretos que la Root CA suscriba con esas terceras partes para asegurar que éstas están obligadas a implementar cualquier control requerido por la Root CA. La Root CA será responsable por la revelación de prácticas relevantes.

b) La Root CA deberá desarrollar la actividades necesarias para la formación y concienciación de los empleados en material de seguridad.

c) La información necesaria para gestionar la seguridad de la Root CA deberá mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado por el foro de gestión de la Root CA.

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

e) La Root CA 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 Root CA haya sido subcontratada a otra organización

6.6.2.2 Clasificación y gestión de información y bienes

La Root CA 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 Root CA 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.

6.6.2.3 Operaciones de gestión

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

a) se protegerá la integridad de los sistemas de la Root CA 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 Root CA 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 Root CA serán separadas de las operaciones normales

6.6.2.4 Gestión del sistema de acceso

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

AC General

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

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

c) La Root CA 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 Root CA 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 Root CA será identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de certificados.

f) El personal de la Root CA será responsable de sus actos.

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 y revocación

g) Las instalaciones de la Root CA 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.

6.6.2.5 Gestión del ciclo de vida del hardware criptográfico

La Root CA 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 Root CA activada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo

6.6.3 Evaluación de la seguridad del ciclo de vida

No estipulado

6.7. Controles de seguridad de la red

Ya definido

6.8. *Controles de ingeniería de los módulos criptográficos*

Todas las operaciones criptográficas de la Root CA 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 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL 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

Las extensiones de los certificados proporcionan información sobre los atributos técnicos del propio certificado, así como cierta información de tipo personal o profesional del suscriptor y emisor del certificado, lo que permitirá formar la confianza del usuario.

El estándar x.509 está formado por extensiones fijas pero también por extensiones propias a las cuales el emisor hace referencia por medio de su OID.

Version	V3
Algoritmo de Firma	Sha1WithRsaSignature
Emisor (Issuer)	CN = Global Chambersign Root OU = http://www.chambersign.org O = AC Camerfirma SA - CIF A82743287 C = EU
Asunto (Subject)	CN = Global Chambersign Root OU = http://www.chambersign.org O = AC Camerfirma SA - CIF A82743287 C = EU
Periodo de Validez	25 años
Algoritmo de Clave Publica	RsaEncryption

Tamaño de Clave Publica	2048
Uso de clave	Firma de certificados, Firma CRL sin conexión, Firma CRL
Punto de distribución de CRL	Http://crl.chambersign.org/chambersignroot.crl
Restricciones Básicas	**CA**: **PathLenConstraint**: 10
identificador de clave autoridad	Id. de clave DN Emisor de certificado: Número de serie del certificado de emisor
Nombre alternativo del emisor	chambersignroot@chambersign.org
Nombre alternativo del sujeto	chambersignroot@chambersign.org
Políticas de Certificado	OID 1.3.6.1.4.1.17326.10.1.1 Declaración del Emisor: This Root CA is designed to stablish trust for a PKI intended to issue qualified certificates, mainly. According to DIRECTIVE 1999/93/EC OF EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999, advanced electronic signatures wich are based on a qualified certificate and wich are created by a secure-signature-creation device satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data and are admissible as evidence in legel proceedings. Therefore, qualified certificates under this root CA don't require further recognition and can be used at the sole discretion of the user. Further information at http://www.chambersign.org/root-chambersign/use.html
Uso de clave extendido	Correo seguro Autenticación del cliente Autenticación del servidor Firma de código

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será descrito en la declaración de prácticas del emisor y estará alineado con las garantías criptográficas marcadas por las normativas técnicas y jurídicas aplicables

7.1.4 Restricciones de los nombres

No estipulado

7.2. Perfil de CRL

Las extensiones de los certificados de la lista de certificados revocados proporcionan información sobre el archivo contenedor de las revocaciones concretos, tales como el emisor de la CRL o el periodo de validez de la misma. Esta información, al igual que la de los certificados permitirá formar la confianza del usuario.

El estándar x.509 está formado por extensiones fijas pero también por extensiones propias a las cuales el emisor hace referencia por medio de su OID.

Version	V2
Emisor	CN = Global Chambersign Root OU = http://www.chambersign.org O = AC Camerfirma SA - CIF A82743287 C = EU
Periodo máximo de valide	1 año
Algoritmo de firma	En Prácticas de certificación
identificador de clave de autoridad	Id. de clave DN Emisor de certificado: Número de serie del certificado de emisor

7.2.1 Número de versión

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

7.2.2 CRL y extensiones

No estipulado

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 del emisor.

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

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

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

Si un cambio en la política afecta de manera relevante a un número significativo de usuarios 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 la dirección del emisor

8.4. Procedimientos de aprobación de la CPS

La aprobación y autorización de una AC delegada y sus políticas de certificación deberán respetar los procedimientos especificados la presente política y por la PA. Las partes de la política de certificación o CPS de una AC delegada 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

ARL *Authority Revocation List.* Lista de certificados revocados de AC's delegadas

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

AC Delegada	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, vinculando una determinada clave pública con una persona.
AC Root (CA Root)	Es la entidad responsable de la emisión, y revocación de los certificados digitales para la AC Delegada.
ARL	Es la lista que contiene los certificados de AC's delegadas revocados
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 practicas 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
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.
Usuario	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: 03.09.2018 13:03:32
Camerfirma Certificado Digital