DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES **AC CAMERFIRMA SA**

(Certificados No Cualificados)

Versión 3.3.6

Idioma: **Castellano**

FRANCE MARIE SYLVIA VIDAL LECA
Firmado digitalmente por FRANCE MARIE SYLVIA VIDAL LECA
Fecha: 2020.08.04 14:40:08 +02'00'

RAMIRO MUÑOZ MUÑOZ
Firmado digitalmente por RAMIRO MUÑOZ MUÑOZ
Fecha: 2020.08.04 15:15:52 +02'00'

Índice de Contenido

Contenido

1. INTRODUCCIÓN *9*

1.1. Visión General **9**

1.2. Identificación y nombre del documento **10**

1.3. Participantes en la PKI **11**

1.3.1 Autoridades de Certificación 11

1.3.2 Autoridades de Registro 11

1.3.3 Firmante/Suscriptor 13

1.3.4 Parte que confía 13

1.3.5 Otros participantes 13

1.4. Ámbito de aplicación y usos **29**

1.4.1 Usos apropiados de los certificados 29

1.4.2 Usos prohibidos de los certificados 29

1.5. Autoridad de Políticas **30**

1.5.1 Organización que administra el documento 30

1.5.2 Datos de contacto de la organización 30

1.5.3 Persona que determina la idoneidad de CPS para la política 30

1.5.4 Procedimientos de gestión del documento 31

1.6. Acrónimos y Definiciones. **31**

1.6.1 Acrónimos 31

1.6.2 Definiciones 32

2. RESPONSABILIDAD DE PUBLICACIÓN Y REPOSITORIOS *35*

2.1. Repositorios **35**

2.2. Publicación de información de certificados **35**

2.2.1 Políticas y Prácticas de Certificación. 36

2.2.2 Términos y condiciones. 36

2.2.3 Difusión de los certificados. 36

2.3. Frecuencia de publicación. **36**

2.4. Controles de acceso a los repositorios. **37**

3. IDENTIFICACIÓN Y AUTENTICACIÓN *38*

3.1. Denominación **38**

3.1.1 Tipos de nombres 38

3.1.2 Significado de los nombres 38

3.1.3 Anonimato o pseudónimos de suscriptores 38

3.1.4 Reglas utilizadas para interpretar varios formatos de nombres 38

3.1.5 Unicidad de los nombres 39

3.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos 39

3.1.7 Procedimiento de resolución de disputas de nombres 39

3.2. Validación inicial de la identidad **40**

3.2.1 Métodos de prueba de la posesión de la clave privada. 40
3.2.2 Identificación de la entidad 40
3.2.3 Identificación de la identidad de un individuo. 42
3.2.4 Información de suscriptor no verificada 42
3.2.5 Validación de la autoridad 42
3.2.6 Criterios para la interoperación 45

3.3. Identificación y autenticación de solicitudes de renovación 46
3.3.1 Validación para la renovación rutinaria de certificados 46
3.3.2 Identificación y autenticación de la solicitud de renovación tras una revocación 46

3.4. Identificación y autenticación de la solicitud de revocación 46

4. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS 47

4.1. Solicitud de certificados 47
4.1.1 Quién puede realizar la solicitud de un certificado 47
4.1.2 Procedimiento de alta y responsabilidades 47

4.2. Procesamiento de las solicitudes de certificados 49
4.2.1 Ejecución de las funciones de identificación y autenticación 49
4.2.2 Aprobación o rechazo de la solicitud 49
4.2.3 Plazo para resolver la solicitud 50

4.3. Emisión de certificados 51
4.3.1 Acciones de la CA durante el proceso de emisión 51
4.3.2 Notificación de la emisión al suscriptor 53

4.4. Aceptación de certificados 54
4.4.1 Conducta que constituye aceptación del certificado 54
4.4.2 Publicación del certificado por la AC 54
4.4.3 Notificación de emisión de certificado por la CA a otras entidades 54

4.5. Uso del par de claves y los certificados 55
4.5.1 Uso del certificado y la clave privada del suscriptor 55
4.5.2 Uso de la clave pública y del certificado por la parte que confía 59

4.6. Renovación del certificado 59
4.6.1 Circunstancia para la renovación del certificado 59
4.6.2 Quién puede solicitar renovación 59
4.6.3 Procesamiento de solicitudes de renovación de certificados 60
4.6.4 Notificación de nueva emisión de certificado al suscriptor 60
4.6.5 Conducta que constituye la aceptación de un certificado de renovación 60
4.6.6 Publicación del certificado de renovación por la CA 61
4.6.7 Notificación de emisión de certificado por la CA a otras entidades 61

4.7. Renovación de claves 61
4.7.1 Circunstancia para la renovación de claves (re-key) certificado 61
4.7.2 Quién puede solicitar la certificación de una nueva clave pública 61
4.7.3 Procesamiento de solicitudes de cambio de claves del certificado 61
4.7.4 Notificación de nueva emisión de certificado al suscriptor 61
4.7.5 Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed) 61
4.7.6 Publicación del certificado con renovación de claves (re-keyed) por la AC 62
4.7.7 Notificación de emisión de certificado por la AC a otras entidades 62

4.8. Modificación de certificados 62
4.8.1 Circunstancia para la modificación del certificado 62
4.8.2 Quién puede solicitar la modificación del certificado 62
4.8.3 Procesamiento de solicitudes de modificación de certificados 62
4.8.4 Notificación de la emisión de un nuevo certificado al suscriptor 62
4.8.5 Conducta que constituye la aceptación del certificado modificado 62
4.8.6 Publicación del certificado modificado por la CA 63
4.8.7 Notificación de emisión de certificado por la CA a otras entidades 63

4.9. Revocación y suspensión de certificados 63
4.9.1 Causas de revocación 64
4.9.2 Quién puede solicitar la revocación 65
4.9.3 Procedimiento de solicitud de revocación. 66
4.9.4 Periodo de gracia de la solicitud de revocación 66
4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación 66
4.9.6 Requisitos de comprobación de la revocación por las partes que confían 67
4.9.7 Frecuencia de emisión de CRL's 68
4.9.8 Máxima latencia de CRL 68
4.9.9 Disponibilidad de comprobación on-line de la revocación 68
4.9.10 Requisitos de la comprobación on-line de la revocación 69
4.9.11 Otras formas de divulgación de información de revocación disponibles 69
4.9.12 Requisitos especiales de revocación por compromiso de las claves 69
4.9.13 Circunstancias para la suspensión 69
4.9.14 Quién puede solicitar la suspensión 69
4.9.15 Procedimiento de solicitud de suspensión 70
4.9.16 Límites del periodo de suspensión 70

4.10. Servicios de comprobación del estado de los certificados 70
4.10.1 Características operacionales 70
4.10.2 Disponibilidad del servicio 70
4.10.3 Características opcionales 70

4.11. Finalización de la suscripción 70

4.12. Custodia y Recuperación de Claves 70
4.12.1 Política y prácticas de custodia y recuperación de claves 70
4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión 71

5. CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES 72

5.1. Controles de seguridad física 72
5.1.1 Ubicación y construcción 72
5.1.2 Acceso físico 72
5.1.3 Alimentación eléctrica y aire acondicionado 73
5.1.4 Exposición al agua 73
5.1.5 Prevención y protección de incendios 73
5.1.6 Sistema de almacenamiento. 73
5.1.7 Eliminación de residuos 74
5.1.8 Backup externo 74

5.2. Controles procedimentales 75
5.2.1 Roles de confianza 75
5.2.2 Número de personas requeridas por tarea 76
5.2.3 Identificación y autentificación para cada rol 76

5.2.4 Roles que requieren separación de tareas 77
5.2.5 Arranque y parada del sistema de gestión PKI. 77
5.3. Controles del personal 78
5.3.1 Calificaciones, experiencia y requisitos de autorización 78
5.3.2 Procedimientos de comprobación de antecedentes 79
5.3.3 Requerimientos de formación 79
5.3.4 Requerimientos y frecuencia de la actualización de la formación 79
5.3.5 Frecuencia y secuencia de rotación de tareas 79
5.3.6 Sanciones por acciones no autorizadas 79
5.3.7 Requerimientos de contratación de personal 80
5.3.8 Documentación proporcionada al personal 80
5.4. Procedimientos de registro de eventos 81
5.4.1 Tipos de eventos registrados 81
5.4.2 Frecuencia de tratamiento de registros de auditoria 82
5.4.3 Periodos de retención para los LOGs de auditoria 82
5.4.4 Protección de los registros de auditoría 82
5.4.5 Procedimientos de copia de respaldo de los registros de auditoría 82
5.4.6 Sistema de recogida de información de auditoria 83
5.4.7 Notificación al sujeto causa del evento 83
5.4.8 Análisis de vulnerabilidades 83
5.5. Archivo de registros 83
5.5.1 Tipo de archivos registrados. 83
5.5.2 Periodo de retención para el archivo 84
5.5.3 Protección del archivo 84
5.5.4 Procedimientos de copia de respaldo del archivo 84
5.5.5 Requerimientos para el sellado de tiempo de los registros 84
5.5.6 Sistema de recogida de información de auditoria 85
5.5.7 Procedimientos para obtener y verificar información archivada 85
5.6. Cambio de clave 86
5.7. Recuperación en caso de compromiso de la clave o desastre 86
5.7.1 Procedimientos de gestión de incidencias y compromisos 86
5.7.2 Corrupción de recursos, aplicaciones o datos 86
5.7.3 Compromiso de clave privada de la entidad 87
5.7.4 Continuidad del negocio después de un desastre 87
5.8. Cese de la AC o AR 87
6. CONTROLES DE SEGURIDAD TÉCNICA 88
6.1. Generación e instalación del par de claves 88
6.1.1 Generación del par de claves 88
6.1.2 Entrega de la clave privada al firmante 89
6.1.3 Entrega de la clave pública al emisor del certificado 89
6.1.4 Entrega de la clave pública de la AC a los usuarios 89
6.1.5 Tamaño de las claves 89
6.1.6 Parámetros de generación de la clave pública y control de calidad. 90
6.1.7 Propósitos de uso de claves 90
6.2. Protección de la clave privada y estándares para los módulos criptográficos 90
6.2.1 Controles y estándares de módulos criptográficos 90

6.2.2 Control multipersonal (n de entre m) de la clave privada 91
6.2.3 Depósito de clave privada 91
6.2.4 Copia de seguridad de la clave privada 91
6.2.5 Archivo de la clave privada 92
6.2.6 Introducción de la clave privada en el módulo criptográfico. 92
6.2.7 Almacenamiento de clave privada en el módulo criptográfico 92
6.2.8 Método de activación de la clave privada. 93
6.2.9 Método de desactivación de la clave privada 93
6.2.10 Método de destrucción de la clave privada 93
6.2.11 Calificación del módulo criptográfico 94

6.3. Otros aspectos de la gestión del par de claves 94
6.3.1 Archivo de la clave pública 94
6.3.2 Periodo de uso para las claves públicas y privadas 94

6.4. Datos de activación 95
6.4.1 Generación y activación de los datos de activación 95
6.4.2 Protección de los datos de activación 95
6.4.3 Otros aspectos de los datos de activación 95

6.5. Controles de seguridad informática 95
6.5.1 Requerimientos técnicos de seguridad informática específicos 96
6.5.2 Valoración de la seguridad informática 96

6.6. Controles de seguridad del ciclo de vida 96
6.6.1 Controles de desarrollo del sistema 97
6.6.2 Controles de gestión de la seguridad 97
6.6.3 Evaluación de la seguridad del ciclo de vida 100

6.7. Controles de seguridad de la red 101

6.8. Fuentes de Tiempo 101

7. PERFILES DE CERTIFICADO, CRL Y OCSP 102

7.1. Perfil de Certificado 102
7.1.1 Número de versión 102
7.1.2 Extensiones del certificado 102
7.1.3 Identificadores de objeto (OID) de los algoritmos 102
7.1.4 Formato de Nombres. 102
7.1.5 Restricciones de los nombres 103
7.1.6 Identificador de objeto (OID) de la Política de Certificación 103
7.1.7 Uso de la extensión "Policy Constraints" 103
7.1.8 Sintaxis y semántica de los calificadores de política 103
7.1.9 Tratamiento semántico para la extensión critica "*Certificate Policy*" 103

7.2. Perfil de CRL 104
7.2.1 Número de versión 104
7.2.2 CRL y extensiones 104

7.3. Perfil de OCSP 104
7.3.1 Número de versión 104
7.3.2 Extensiones OCSP 104

8. AUDITORÍAS DE CONFORMIDAD 105

8.1. Frecuencia o circunstancias de las auditorias 105

8.1.1 Auditorías de AC subordinada Externa o certificación cruzada. 106
8.1.2 Auditoria en las Autoridades de Registro 106
8.1.3 Auditorías Internas 106
8.2. Identificación y calificación del auditor 106
8.3. Relación entre el auditor y la AC 107
8.4. Tópicos cubiertos por la auditoria 107
8.5. Acciones tomadas como resultado de las deficiencias 107
8.6. Comunicación de resultados 107
9. ASPECTOS LEGALES Y OTROS ASUNTOS 109
9.1. Tarifas 109
9.1.1 Tarifas de emisión de certificados y renovación. 109
9.1.2 Tarifas de acceso a los certificados. 109
9.1.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados. 109
9.1.4 Tarifas por el acceso al contenido de estas Prácticas de certificación. 109
9.1.5 Política de reintegros. 109
9.2. Responsabilidad financiera 110
9.2.1 Cobertura del Seguro 110
9.2.2 Otros activos 110
9.2.3 Seguro de cobertura o garantía para entidades finales 110
9.3. Confidencialidad de la información del negocio 110
9.3.1 Tipo de información a mantener confidencial 110
9.3.2 Tipo de información considerada no confidencial 110
9.3.3 Responsabilidad de proteger la información confidencial 110
9.4. Privacidad de la información personal 111
9.4.1 Plan de privacidad 111
9.4.2 Información tratada como privada 111
9.4.3 Información no considerada privada 111
9.4.4 Responsabilidad de proteger la información privada 112
9.4.5 Aviso y consentimiento para usar información privada 112
9.4.6 Divulgación de conformidad con un proceso judicial o administrativo 112
9.4.7 Otras circunstancias de divulgación de información 112
9.5. Derechos de propiedad intelectual 113
9.6. Obligaciones y Responsabilidad Civil 113
9.6.1 Obligación y responsabilidad de la CA 113
9.6.2 Obligación y responsabilidad de la RA 115
9.6.3 Obligación y responsabilidad del suscriptor 117
9.6.4 Obligación y responsabilidad de terceras partes 119
9.6.5 Obligación y responsabilidad de otras participantes 119
9.7. Exoneración de responsabilidad 119
9.8. Limitación de responsabilidad en caso de pérdidas por transacciones 121
9.9. Indemnizaciones 121
9.10. Plazo y Finalización 121

9.10.1 Plazo 121
9.10.2 Terminación 121
9.10.3 Efecto de la terminación y la supervivencia 121
9.11. Notificaciones individuales y comunicación con los participantes 121
9.12. Modificaciones 121
9.12.1 Procedimiento de modificación. 121
9.12.2 Mecanismo de notificación y plazos 122
9.12.3 Circunstancias en las que se debe cambiar el OID 122
9.13. Procedimiento de resolución de conflictos 123
9.14. Legislación aplicable 123
9.15. Conformidad con la Ley Aplicable 123
9.16. Otras disposiciones 123
9.16.1 Acuerdo completo 123
9.16.2 Asignación 123
9.16.3 Separabilidad 123
9.16.4 Cumplimiento (honorarios de abogados y exención de derechos) 123
9.16.5 Fuerza mayor 124
9.17. Otras provisiones 124
9.17.1 Publicación y copia de la política 124
9.17.2 Procedimientos de aprobación de la CPS 124
ANEXO I: historia del documento 125

1. INTRODUCCIÓN

1.1. Visión General

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

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

La Declaración de Prácticas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/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 Prácticas de Certificación son distintos, pero aun así es muy importante su interrelación.

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

En definitiva una Política define "qué" requerimientos de seguridad son necesarios para la emisión de los certificados. La Declaración de Prácticas de Certificación nos dice "cómo" se cumplen los requerimientos de seguridad impuestos por la Política.

El presente documento especifica la Declaración de Prácticas de Certificación (en adelante CPS) de AC Camerfirma SA (en adelante, Camerfirma) para la emisión de certificados, y está basada en la especificación de los estándares:

- RCF 3647 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF,
- RFC 3739 3039 Del IETF Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL).
- RFC 6960 Online Certificate Status Protocol - OCSP
- ETSI TS 101 456 V1.2.1 Policy requirements for certification authorities issuing qualified certificate
- ETSI TS 102 042 V1.1.1 Policy requirements for certification authorities issuing public key certificate

- Estas prácticas están alineadas con los requisitos marcados en *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* elaborado por el CA/B Forum http://www.cabforum.org en su versión 1.6.5.

En el caso de que exista alguna inconsistencia entre este documento y los *Baseline Requirements*, los *Baseline Requirements* tendrán prioridad sobre este documento.

Adicionalmente en los requisitos establecidos en las propias políticas de certificación a las que esta CPS da respuesta. Se han tenido también en cuenta las recomendaciones del documento técnico *Security CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*.

Con carácter general, los certificados no cualificados cumplen los requisitos que se prevén en la especificación técnica ETSI TS 102 042, para la política NCP o NCP + cuando se requieren superiores garantías de seguridad.

Por su parte, los certificados cualificados cumplen los requisitos que se prevén en la especificación técnica ETSI TS 101 456, para la política QCP público o QCP + SSCD cuando se emiten conjuntamente con un dispositivo seguro de creación de firma electrónica. Si bien las Autoridades de Certificación y los certificados de usuario final que cubre esta CPS pueden cumplir técnicamente con la especificación técnica ETSI TS 101 456, no se consideran "cualificados" conforme al Reglamento UE Nº910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS), toda vez que no han sido objeto de una Evaluación de conformidad.

Esta CPS se encuentra en conformidad con las Políticas de Certificación de los diferentes certificados emitidos por Camerfirma que vienen descritos en el apartado 1.3.5.8 de esta CPS. En caso de contradicción entre los dos documentos prevalecerá lo dispuesto en este documento.

1.2. Identificación y nombre del documento

Nombre:	CPS Camerfirma SA.
Descripción:	Documento que responde a los requisitos de las Políticas descritas e identificadas en los puntos anteriores de este documento que describen las jerarquías afectadas.
Versión:	Ver página inicial
OID	1.3.6.1.4.1.17326.10.1
Localización:	https://policy.camerfirma.com/

1.3. Participantes en la PKI

1.3.1 Autoridades de Certificación

Es el componente de una PKI responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Firmante (Suscriptor) y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona.

Una Autoridad de certificación (AC) utiliza Autoridades de Registro (AR) para realizar las labores de comprobación de identidad y atributos y almacenamiento de la documentación de los contenidos incorporados en el certificado digital.

Una AC pertenece a una entidad jurídica indicada en el campo organización (O) del certificado digital asociado.

La información relativa a las AC gestionadas por Camerfirma pueden encontrarse en este documento o la dirección Web de Camerfirma http://www.camerfirma.com

Puede existir más de una AC intermedia entre la autoridad de certificación raíz y el certificado de entidad final. El número de AC intermedias permitidas está especificado en la extensión Basic Constraints (pathLenConstraint) del certificado de la Autoridad de Certificación.

1.3.2 Autoridades de Registro

Una AR puede ser una persona física o jurídica que actúa conforme esta CPS y, en su caso, mediante un acuerdo suscrito con una AC concreta, ejerciendo las funciones de gestión de las solicitudes, identificación y registro de los solicitantes del certificado y aquellas que se dispongan en las Políticas de Certificación concretas. Las AR son autoridades delegadas de la AC, aunque ésta es la última responsable del servicio en última instancia.

Bajo las presentes prácticas se reconocen los siguientes tipos de AR:

- AR Cameral: Aquellas gestionadas directamente o bajo el control de una Cámara de Comercio.
- AR Empresarial: Aquella gestionada por una organización pública o una entidad privada para la distribución de certificados a sus empleados.
- AR Remota: Autoridad de Registro gestionada en una localización remota que se comunica con la plataforma mediante la capa de WebServices de STATUS.

PVP. Punto de Verificación Presencial que depende siempre de una AR y actúa bajo su control y supervisión. Su principal misión es la de cubrir la evidencia de la personación del solicitante, y de la entrega de documentación a la AR la cual la validará según la Política aplicable para tramitar la solicitud de emisión del certificado. Para esas funciones los PVP no están sujetas a formación previa, pero podrá ser objeto de controles puntuales.

En ocasiones, el PVP podrá ver ampliadas sus funciones a las de cotejo de documentación entregada, comprobación de su idoneidad respecto al tipo de certificado solicitado, así como a la entrega en caso de tarjeta criptográfica del certificado al solicitante, pero no podrá nunca validar los certificados.

A los efectos de la presente CPS podrán actuar como AR:

Para la Jerarquía Chambers of Commerce Root:

- La propia Autoridad de Certificación.
- Las Cámaras de Comercio, Industria y Navegación ó aquellas entidades delegadas por éstas. El proceso de registro puede ser realizado por parte de diferentes entidades delegadas.
- Las Autoridades de Registro Empresariales (AR Empresarial), como entidades delegadas de una AR, a la que se vinculan contractualmente, para llevar a cabo los registros completos de Firmantes/Suscriptores dentro de una determinada organización o demarcación. Con carácter general, los operadores de dichas AR Empresariales gestionarán únicamente las solicitudes y los certificados en el ámbito de su organización o demarcación, salvo que se determine de otro modo por la AR de la que dependen. Por ejemplo, los empleados de una corporación, los asociados de una agrupación empresarial, los colegiados de un colegio profesional.
- Adicionalmente la Administración Pública, en el caso de los certificados emitidos bajo la AC Camerfirma AAPP.
- A su vez, cualquier AR puede delegar en los Puntos de Verificación Presencial (PVP) la función de verificación presencial del titular del certificado y la recogida de documentación, y en su caso de cotejo de documentación y verificación de su idoneidad así como entrega de material. Habida cuenta que no tienen capacidad de registro, se vinculan contractualmente con una AR mediante un contrato tipo proporcionado por Camerfirma. En base a la documentación suministrada por el PVP, el operador de la AR comprueba la documentación, y en su caso, da curso a la emisión del certificado por la AC sin necesidad de realizar nueva verificación presencial. El contrato define las funciones delegadas por la AR en el PVP.

Para la Jerarquía Chambersign.

- La propia Autoridad de Certificación.
- Cualquier agente nacional o internacional que mantenga una relación contractual con la AC y supere los procesos de alta y las Auditorias exigidas en las Políticas de Certificación.

De igual forma que en la jerarquía Chambers of Commerce Root, las AR pueden delegar en los Puntos de Verificación Presencial (PVP) ciertas funciones no de registro como la verificación presencial del titular del certificado.

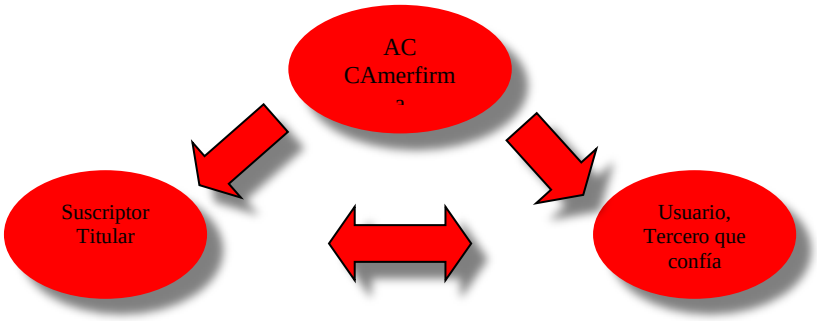
En ningún caso se permite la delegación de la validación de dominios en la emisión de certificados de Servidor Seguro.

1.3.3 Firmante/Suscriptor

Entendemos por Firmante/Suscriptor al titular del certificado cuando éste sea una persona física o jurídica y viene descrita en el campo CN del certificado. Cuando se emita a nombre de un dispositivo hardware o aplicativo informático, se considerará Firmante/Suscriptor, la persona física o jurídica solicitante del certificado emitido.

1.3.4 Parte que confía

En esta CPS se entiende por Tercero que confía o usuario, la persona que recibe una transacción electrónica realizada con un certificado emitido por cualquiera de las AC de Camerfirma y que voluntariamente confía en el Certificado emitido por ésta. Grafico.



1.3.5 Otros participantes

1.3.5.1 Autoridad de Certificación Intermedia o subordinada (SubCA) .

Una Autoridad de Certificación Intermedia (SubCA) es un objeto jerárquico que obtiene un certificado de la AC Raíz para emitir certificados de entidad final u otros certificados de AC.

Las SubCAs permiten distribuir riesgos en una estructura jerárquica compleja, permitiendo a ésta última gestionar por ejemplo sus claves en un entorno "en línea" más ágil, protegiendo las claves de la AC Raíz almacenadas en un entorno seguro desconectado. Una SubCA permite la organización de diferentes tipos de certificados emitidos por la AC principal.

El certificado de una SubCA es firmado por una root CA (entidad raíz origen de la jerarquía de certificación) u otra SubCA.

Una SubCA puede ser objeto de limitaciones por la AC de la cual depende jerárquicamente. Técnicamente mediante una combinación de los siguientes parámetros dentro del certificado: Extended Key Usage y Name constrains adicionalmente a aquellas establecidas contractualmente.

Una Autoridad intermedia puede identificarse como interna o externa. Una SubCA Interna es propiedad de la misma organización que la AC de la que depende jerárquicamente en este caso AC Camerfirma. Por el contrario, una SubCA externa es propiedad de una organización distinta, que ha solicitado incorporarse a la jerarquía de la AC de la que depende jerárquicamente y puede usar o no una infraestructura técnica distinta a la empleada por esta.

1.3.5.2 Entidad de Acreditación

La entidad de acreditación será el órgano gestor correspondiente que admite, acredita y supervisa las entidades de certificación, incluso cuando no ha sido objeto de una Evaluación de Conformidad. Esta tarea recae en el Ministerio de Asuntos Económicos y Transformación Digitaldel Gobierno de España, siendo la autoridad competente dependiendo del Estado Español miembro de la Unión Europea , de acuerdo con la legislación dictada en cumplimiento del Reglamento (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS) l

Las SubCAs que desarrolla Camerfirma pueden estar sujetas a marcos jurídicos de distintos países o regiones, recayendo la entidad de Acreditación, en estos casos, en los organismos nacionales correspondientes.

- Para España: Ministerio de Asuntos Económicos y Transformación Digital
- Para Andorra: Ministeri d'Economia y Territori del Govern d'Andorra

1.3.5.3 Prestador de servicios de confianza (PSC).

Entendemos bajo la presente CPS, a un PSC como aquella entidad, tercera parte de confianza, que presta los servicios concretos relativos al ciclo de vida de los certificados y que puede gestionar directa o indirectamente, una o más Autoridades de Certificación y servicios asociados como la emisión de sellos de tiempo, provisión de dispositivos de firma o servicios de validación.

Bajo esta CPS, los servicios de confianza que presta el PSC Camerfirma son no cualificados conforme al Reglamento eIDAS, al no haber sido objeto de una evaluación de conformidad.

AC Camerfirma emite certificados de SubCA a terceros para su acreditación dentro y fuera del marco jurídico español, pudiendo ser estos terceros considerados como PSC en dichos países ante sus entidades de Acreditación nacionales.

1.3.5.4 Entidad.

La Entidad se constituye como aquella organización, de carácter público o privado, individual o colectivo, reconocido en derecho, con la que el Firmante/Suscriptor mantiene una vinculación determinada que aparece definida en el campo (O) ORGANIZACIÓN de cada certificado.

Y así

- En el caso del certificado de persona física, de empleado público de vinculación, de Certificat d´actuació de PERSONA FÍSICA al servei de l´ADMINISTRACIÓ, de Certificat d'actuació de PERSONA FÍSICA al servei d'una ORGANITZACIÓ, Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL COL·LEGIAT, la Entidad se encuentra vinculada al Firmante/Suscriptor mediante una relación mercantil, laboral, colegial, etc.

- En el caso del certificado de Representante, Certificat d'actuació de REPRESENTANT PERSONA JURÍDICA, la Entidad se encuentra representada con amplios poderes por el Firmante/Suscriptor.

- .

- En el caso del certificado de Apoderamiento Especial, la Entidad se encuentra representada para determinados trámites por el Firmante/Suscriptor.

- En el caso del certificado de Facturación electrónica, la Entidad autoriza al Firmante/Suscriptor para que realice la facturación electrónica de la misma.

- En el caso de certificados de Servidor Seguro/Sello electrónico/ Sello Electrónico en QSCD/, Sede electrónica, Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica), Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic, la Entidad es la titular del dominio de Internet o del aplicativo para el cual se ha pedido el certificado.

Como norma general la Entidad queda identificada dentro del certificado en el campo organización (O) y su identificador fiscal en un campo propietario del certificado. Para más información ver el apartado 3.1.1.

1.3.5.5 Solicitante

Se entenderá por Solicitante la persona física que realiza la petición de emisión del Certificado al PSC, bien sea directamente o a través de un representante autorizado.
Pueden ser solicitantes:

- La persona que será el futuro firmante del certificado.
- Un representante de la organización bajo la cual se emitirá el certificado.
- Una persona autorizada por el futuro suscriptor/firmante del certificado.
- Una persona autorizada por la Entidad de Registro.
- Una persona autorizada por la Entidad de Certificación.

1.3.5.6 Responsable de certificados /Poseedor de las claves

Para los certificados emitidos a personas físicas, esta CPS considera responsable al titular del certificado (el firmante/suscriptor).

Para los certificados emitidos a personas jurídicas (Sello electrónico/Servidor seguro), esta CPS considera responsable a la persona física que realiza la solicitud (El solicitante) que debe estar identificado dentro del certificado, incluso si se efectúa la solicitud a través de un tercero, cuando ésta tenga conocimiento de la existencia del certificado.

Para los certificados de componente esta CPS considera responsable a la persona física que realiza la solicitud en su propio nombre o a través de a un tercero.

1.3.5.7 Usuario Final

Los usuarios finales son las personas que obtienen y utilizan certificados personales, de entidad, de dispositivos y de objetos emitidos por las Entidades de Certificación, y, en concreto, podemos distinguir los siguientes usuarios finales:

- Los solicitantes de certificados.
- Los suscriptores o titulares de certificados.
- Los poseedores de claves.

- Los verificadores de firmas y certificados.

1.3.5.8 Jerarquías

En este apartado presentaremos las jerarquías y Autoridades de Certificación (en adelante AC o ACs) que gestiona Camerfirma. La utilización de jerarquías permite reducir los riesgos asociados a la emisión de certificados y organizarlos en diferentes ACs.

Todas las Autoridades de Certificación (AC) descritas pueden emitir certificados de respondedor OCSP. Este certificado servirá para firmar y verificar las respuestas del servicio OCSP sobre el estado de los certificados emitidos por estas AC.

Camerfirma gestiona dos estructuras jerarquizadas:

- Chambers of Commerce Root.
- Global Chambersign Root.

Como característica general los nombres de las AC en los certificados emitidos para estas se irán modificando según lleguen a su fecha de caducidad, incorporando el año de su emisión. Por ejemplo, podemos encontrarnos con que el nombre de la AC "AC Express Corporate Server" cambie a "AC Express Corporate Server 2009". No obstante, su OID y sus características seguirán siendo las mismas, a no ser que así se indique en esta CPS.

1.3.5.8.1 Emisión de certificados de pruebas.

Camerfirma emite con objeto de que tanto el organismo regulador en procesos de inspección o registro de nuevos certificados, como los desarrolladores de aplicaciones en proceso de integración o de evaluación para su aceptación, certificados de la jerarquía real pero con datos ficticios. Camerfirma incorpora en dichos certificados la siguiente información de forma que el tercero que confía pueda valorar claramente que se trata de un certificado de pruebas sin responsabilidad:

Nombre de la entidad	[SOLO PRUEBAS] ENTIDAD
NIF Entidad	R05999990
Domicilio (calle/número) de la entidad	DOMICILIO
Código Postal	5001
Teléfono contacto	902361207
Nombre	JUAN
Primer Apellido	CÁMARA
Segundo Apellido	ESPAÑOL
DNI/NIE	00000000T

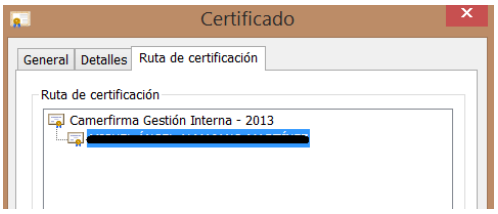
En casos donde el proceso de homologación, evaluación…. necesita la emisión de un certificado de pruebas con datos reales, el proceso se realiza después de la firma de un acuerdo de confidencialidad con el organismo encargado de hacer las tareas de homologación o evaluación. Los datos serán los específicos de cada cliente, pero delante del nombre de entidad siempre se pondrá [SOLO PRUEBAS] para poder identificar a primera vista que se trata de un certificado de pruebas sin responsabilidad.

Bajo esta CPS no se emiten certificados de pruebas para servidor seguro.

1.3.5.8.2 Jerarquía Camerfirma Gestión Interna.

Camerfirma ha desarrollado una autoridad de certificación especial para la emisión de certificados de operador de Autoridad de Registro. Con este certificado un operador podrá realizar las gestiones propias de su rol en la plataforma de gestión de Camerfirma STATUS®.

Esta jerarquía está compuesta por una única AC que emite certificado de entidad final.



Como diseño general en el nombre del titular del certificado de las AC que emite Camerfirma, se incorporan al final el año de creación de las claves criptográficas asociadas, realizándose su modificación al año correspondiente, en cada proceso de renovación del certificado

1.3.5.9 Jerarquía Chambers of Commerce Root.

Esta Jerarquía está diseñada para desarrollar una red de confianza que tiene por objeto fundamental la emisión de certificados digitales de identidad empresarial y donde las Autoridades de Registro (en adelante AR o AR´s) son gestionadas por las Cámaras de Comercio, Industria y Navegación de España o entidades públicas o privadas asociadas a éstas.

Resumiendo, las características de esta jerarquía son:

- Ámbito Geográfico Español. (salvo excepciones)
- Autoridades de Registro gestionadas por Cámaras de Comercio.
- Ámbito Empresarial.

Esta jerarquía incorpora Autoridades de Certificación intermedias que emiten certificados digitales en diferentes entornos:

Chambers of Commerce Root	
AC Camerfirma Express Corporate Server	1.3.6.1.4.1.17326.10.11.1
AC Camerfirma Certificados Camerales	1.3.6.1.4.1.17326.10.9.1
Certificado de pertenencia a empresa	1.3.6.1.4.1.17326.10.9.2
Certificado de representante	1.3.6.1.4.1.17326.10.9.3
Certificado de apoderado	1.3.6.1.4.1.17326.10.9.5
Certificado de Representante para trámites con las AAPP (hasta el 8 de junio de 2020)	*1.3.6.1.4.1.17326.10.16.1.3.2*
Certificado de Cifrado (Software)	1.3.6.1.4.1.17326.10.9.6

Certificado de Factura electrónica	1.3.6.1.4.1.17326.10.9.7
AC CAMERFIRMA AAPP	1.3.6.1.4.1.17326.1.3.1
Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto	1.3.6.1.4.1.17326.1.3.3.1
Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio	1.3.6.1.4.1.17326.1.3.3.2
Certificado reconocido de empleado público, nivel alto, firma	1.3.6.1.4.1.17326.1.3.4.1
Certificado reconocido de empleado público, nivel alto, autenticación.	1.3.6.1.4.1.17326.1.3.4.2
Certificado reconocido de empleado público, nivel alto, cifrado	1.3.6.1.4.1.17326.1.3.4.3
Certificado reconocido de empleado público, nivel medio	1.3.6.1.4.1.17326.1.3.4.4
Chambers of Commerce Root - 2008	
AC CAMERFIRMA AAPP II - 2014	1.3.6.1.4.1.17326.1.3.1
Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto	1.3.6.1.4.1.17326.1.3.3.1
Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio	1.3.6.1.4.1.17326.1.3.3.2
Certificado reconocido de empleado público, nivel alto, firma	1.3.6.1.4.1.17326.1.3.4.1
Certificado reconocido de empleado público, nivel alto, autenticación.	1.3.6.1.4.1.17326.1.3.4.2
Certificado reconocido de empleado público, nivel alto, cifrado	1.3.6.1.4.1.17326.1.3.4.3
Certificado reconocido de empleado público, nivel medio	1.3.6.1.4.1.17326.1.3.4.4
Camerfirma Codesign II - 2014	AnyPolicy
De firma de código	1.3.6.1.4.1.17326.10.12.2
Camerfirma TSA - 2013	AnyPolicy
TSU-2 Claves en SW almacenadas en HW. SmartTSU	1.3.6.1.4.1.17326.10.13.1.2
Sello de tiempo TSU-2	1.3.6.1.4.1.17326.10.13.1.2.1
TSU-3 Claves en HW con acceso autenticado al servicio.	1.3.6.1.4.1.17326.10.13.1.3
Sello de tiempo TSU-3	1.3.6.1.4.1.17326.10.13.1.3.1
Camerfirma TSA II - 2014	AnyPolicy
TSU-2 Claves en SW almacenadas en HW. SmartTSU	1.3.6.1.4.1.17326.10.13.1.2
Sello de tiempo TSU-2	1.3.6.1.4.1.17326.10.13.1.2.1
TSU-3 Claves en HW con acceso autenticado al servicio.	1.3.6.1.4.1.17326.10.13.1.3
Sello de tiempo TSU-3	1.3.6.1.4.1.17326.10.13.1.3.1
De Respondedor OCSP	1.3.6.1.4.1.17326.10.9.8

1.3.5.9.1 AC Camerfirma Express Corporate Server.

Es una AC intermedia que emitió certificados digitales cuyos titulares eran máquinas o aplicativos.

Todos los certificados que emitió caducaron antes de la redacción de esta versión de la CPS.

1.3.5.9.2 AC Camerfirma Certificados Camerales.

"AC Camerfirma Certificados Camerales" es una Autoridad de Certificación multi-política, que emite certificados no cualificados conforme a eIDAS, de vinculación empresarial dentro del territorio español, conformes los criterios establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica y cuyas funcionalidades se describen a continuación.

Los certificados finales se dirigen a:

1.3.5.9.2.1 Personas físicas con atributo de vinculación a Entidad.

1.3.5.9.2.1.1 Certificado de pertenencia a empresa

Determinan la relación de vinculación (laboral, mercantil, colegial, etc.) entre una persona física (titular del certificado/firmante/suscriptor) y una Entidad (campo organización del certificado).

1.3.5.9.2.1.2 Certificado de representante

Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/firmante/suscriptor) y una Entidad (descrita también en el campo Organización del certificado).

1.3.5.9.2.1.3 Certificado de apoderado

Determina la relación de representación específica o de apoderamiento especial (con facultades limitadas) entre una persona física (titular del certificado/firmante/suscriptor) y una Entidad (descrita también en el campo Organización del certificado).

1.3.5.9.2.1.4 Certificado de Representante de Persona Jurídica para trámites con las AAPP (a partir del 9 de jnio de 2020, pasa a ser regulado por la CPS – eIDAS de Camerfirma)

Determina la relación de representación legal entre la persona física (titular del certificado/firmante/suscriptor) y una Entidad con personalidad jurídica (descrita también en el campo Organización del certificado) en un dispositivo seguro de creación de firma

1.3.5.9.2.1.5 Certificado de Representante de Entidad Sin Personalidad Jurídica para trámites con las AAPP (a partir del 9 de junio de 2020, pasa a ser regulado por la CPS - eIDAS de Camerfirma)

Determina la relación de representación legal entre la persona física (titular del certificado/firmante/suscriptor) y una Entidad sin personalidad jurídica (descrita también en el campo Organización del certificado

.

1.3.5.9.2.2 Certificado de Factura electrónica

La emisión de Factura electrónica ha sido uno de los motores que han potenciado el uso de los certificados electrónicos. La Agencia tributaria regula el uso de los certificados electrónicos en el Real Decreto 1496/2003. Para realizar una Factura electrónica es necesario firmar el documento electrónico con un certificadoelectrónico. Camerfirma crea con el certificado de factura un elemento adaptado a las necesidades específicas de la facturación electrónica. El certificado está emitido a una persona física autorizada expresamente por la Entidad para ello con una limitación de uso para la emisión de Factura electrónica.

1.3.5.9.2.3 Certificado de Cifrado (Software)

El certificado de cifrado es un certificado técnico que permite el uso exclusivo de cifrado de datos.

Los certificados de persona física de pertenencia a entidad, de representante, de apoderamiento especial, de facturación electrónica anteriormente descritos permiten el uso de la clave para el cifrado de datos, pero Camerfirma no custodia ni almacena las claves privadas de los titulares de los certificados cumpliendo así los requerimientos de la Ley 59/2003 de Firma Electrónica, de 19 de diciembre. En esta situación si el titular del certificado o, , el custodio del certificado perdiera el control sobre la clave privada, perdería también el acceso a todos los datos cifrados con la clave pública asociada.

El certificado de cifrado permite al prestador de los servicios, es decir en este caso Camerfirma, custodiar la clave privada del titular del certificado para reponerla en caso de pérdida.

1.3.5.9.3 AC Camerfirma AAPP.

Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) establecía en el Capítulo Segundo, Título Segundo, los mecanismos de aplicación por las Administraciones Públicas (AAPP) para la identificación y firma electrónica basada en certificados electrónicos (hoy sustituida por las Leyes 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público.).

Dentro de la LAECSP (y ahora dentro de las Leyes 39/2015 y 40/2015) se establecían diversas soluciones a múltiples problemas existentes actualmente en el ámbito de la identificación y firma electrónica de las Administraciones Públicas, entre ellas, hacia los ciudadanos y empresas, y con sus empleados públicos.

La Administración General del Estado ha definido un modelo de certificación donde se combina la existencia de prestadores públicos de servicios de certificación con la posibilidad que organismos dependientes de la Administración General del Estado (AGE) puedan contratar prestadores privados de servicios de certificación.

Dicho modelo contempla una disposición mixta, tratándose de un modelo de libre mercado regulado, en la que prestadores de servicios de certificación privados podrían ser contratados por algún organismo dependiente de la AGE para prestarle servicios de certificación.

AC Camerfirma en base a lo anterior y bajo el esquema de identificación y firma de la AGE y específicamente su política de certificación, emitía (y seguirá emitiendo bajo petición expresa del cliente/AAPP) los siguientes tipos de certificados (no cualificados eIDAS):

- Certificado electrónico de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto.
- Certificado electrónico de sello electrónico de Administración, órgano o entidad de derecho público, nivel medio.
- Certificado electrónico de Empleado Público, nivel alto, firma.
- Certificado electrónico de Empleado Público, nivel alto, autenticación.
- Certificado electrónico de Empleado Público, nivel alto, cifrado.
- Certificado electrónico de Empleado Público, nivel medio.

1.3.5.9.4 Firma de Código.

Los certificados emitidos por esta AC, tendrán continuidad con los mismos OID en la AC "Camerfirma AC CodeSign – AAAA". Siendo AAAA el año de emisión del certificado.

AC intermedia llamada "Camerfirma CodeSign" que emite certificados para la firma de código. Los certificados para la firma de código permiten, como su nombre indica, que los desarrolladores apliquen una firma electrónica sobre el código que desarrollan: ActiveX, applets java, macros para Microsoft Office, etc. estableciendo de esta forma, en dicho código, garantías de integridad y autenticidad.

1.3.5.9.5 Sellos de tiempo.

Los certificados emitidos por esta AC, tendrán continuidad con los mismos OID en la AC "Camerfirma TSA – AAAA". Siendo AAAA el año de emisión del certificado.

La tercera Autoridad intermedia "AC Camerfirma TSA" está destinada a emitir certificados para la emisión de sellos de tiempo. Un sello de tiempo es un paquete de datos con una estructura estandarizada donde se asocia el código resumen o código HASH de un documento o transacción electrónica a una fecha y hora concreta.

La autoridad de sellado de tiempo emite certificados a entidades intermedias llamadas "Unidades de Sellado de Tiempo" TSU. Estas unidades de sellado son las que finalmente emiten los sellos de tiempo ante la recepción de una solicitud estandarizada que siga las especificaciones del RFC 3161. Cada una de estas TSU puede estar asociada, bien a unas características técnicas del servicio específicas, bien a un uso exclusivo de un cliente.

Los certificados de TSU tienen una duración de 6 años y un uso de clave privada de 1 año, de tal forma que los certificados de tiempo emitidos por estas TSU tengan una duración mínima de 5 años.

Bajo esta DPC se permite la emisión de certificados de TSU a empresas y organismos que residan fuera de territorio español. El procedimiento de emisión del certificado se tratará en el apartado correspondiente de esta DPC.

AC Camerfirma emite certificados de TSU en equipos homologados por AC Camerfirma. Los equipos homologados se publicarán en la web de Camerfirma. Los equipos homologados pueden estar localizados en las instalaciones del suscriptor bajo la firma de una declaración responsable y el cumplimiento de los requisitos asociados a la emisión de un certificado de TSU.

AC Camerfirma emite también certificados de TSU para almacenarse en plataformas de terceros siempre que dichas plataformas:

- Se sincronicen con las fuentes de tiempo marcadas por Camerfirma.
- Permitan la auditoria de sus sistemas por parte Camerfirma o un tercero autorizado.
- Permitan el acceso a su servicio de sellado a los aplicativos de AC Camerfirma con el objeto de establecer los controles correspondientes respecto a la corrección de la marca de hora.
- Firmen un acuerdo de servicio.
- Permitan el acceso a AC Camerfirma para recopilar información de los sellos emitidos o bien envíen un informe periódico sobre el número de sellos emitidos.
- Presenten un acta de creación de las claves en un entorno seguro tal como indican las políticas de certificación de TSA de Camerfirma (HSM certificado FIPS 140-1 Nivel 2) firmado por una organización competente. Esta acta será previamente valorado y firmado por personal técnico de AC Camerfirma antes de darle validez.

Las políticas de los certificados de TSU son:

1.3.5.9.5.1 OID 1.3.6.1.4.1.17326.10.13.1.2

Las claves se generan y se almacenan en una batería de tarjetas criptográficas certificadas EAL4+ CWA 14169. El proceso de creación y almacenamiento de claves queda registrado en el departamento de sistemas, encargado de realizar estas operaciones.

El acceso al servicio es autenticado por usuario/contraseña o por certificado digital. Se permite también las implantaciones de autenticación por IP.

1.3.5.9.5.2 OID 1.3.6.1.4.1.17326.10.13.1.3

Las claves se generan y almacenan en un HSM FIPFS 140-1 certificado nivel 2 o superior.

El acceso al servicio es autenticado por usuario/contraseña o por certificado digital. Se permite también las implantaciones de autenticación por IP.

1.3.5.10 Jerarquía Global Chambersign ROOT.

Esta Jerarquía está creada para la emisión de certificados bajo proyectos concretos con una/s determinada/s Entidad/es. Por este motivo, es una jerarquía abierta donde los certificados y la gestión de los mismos se ajustan a las necesidades concretas de un proyecto. En este sentido, y a diferencia de la "Chambers of Commerce Root" anteriormente expuesta, las Autoridades de Registro no tienen por qué encontrarse enmarcadas dentro del ámbito de las Cámaras de Comercio Españolas, ni en un ámbito territorial concreto, ni un ámbito empresarial o de vinculación a entidad.

Global Chambersign Root puede emitir también certificados de SubCA a entidades terceras bajo las condiciones descritas en los apartados correspondientes de esta DPC.

El objeto de esta jerarquía es desarrollar un modelo replicable en diferentes países.

Las características principales de esta jerarquía son:

- Ámbito Geográfico NO restringido
- Autoridades de Registro NO restringidas.
- Ámbito NO restringido a una relación de empresa.

En el marco de esta Jerarquía se desarrollan distintas Autoridades de Certificación intermedias que corresponderán a marcos nacionales distintos. La primera Autoridad intermedia corresponde a AC Camerfirma SA (España) y dentro de esta la Autoridad de certificación:

Global Chambersign Root	
AC Camerfirma	AnyPolicy
RACER	AnyPolicy
Certificado de Persona Física de Vinculación Pertenencia	1.3.6.1.4.1.17326.10.8.2
Certificado de Persona Física de Vinculación Representación	1.3.6.1.4.1.17326.10.8.3
Certificado de Persona Física Ciudadano Emprendedor	1.3.6.1.4.1.17326.10.8.6
Certificado de Persona Física de Vinculación Factura Electrónica	1.3.6.1.4.1.17326.10.8.7
Certificado de Persona Física de Vinculación Apoderado	1.3.6.1.4.1.17326.10.8.8
PERSONA FÍSICA en DSCF – SIGNATURA	2.16.20.2.1.3.1.1.3
PERSONA FÍSICA en DSCF – IDENTITAT	2.16.20.2.1.3.1.1.1
PERSONA FÍSICA en programari	2.16.20.2.1.3.1.1.2
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PERSONA FÍSICA PROFESSIONAL en programari	2.16.20.2.1.3.1.12.2
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	2.16.20.2.1.3.1.12.2
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.4.3
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.4.1

PERSONA FÍSICA al servei d'una ORGANITZACIÓ en programari	2.16.20.2.1.3.1.4.2
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.5.3
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.5.1
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ en programari	2.16.20.2.1.3.1.5.2
SEGELL D'EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	2.16.20.2.1.3.1.2.3
SEGELL D'EMPRESA (Persona Jurídica) en HSM – IDENTITAT	2.16.20.2.1.3.1.2.1
SEGELL D'EMPRESA (Persona Jurídica) en programari	2.16.20.2.1.3.1.2.2
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	2.16.20.2.1.3.1.3.3
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	2.16.20.2.1.3.1.3.1
REPRESENTANT PERSONA JURÍDICA en programari	2.16.20.2.1.3.1.3.2
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en HSM	2.16.20.2.1.3.1.8.3
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en programari	2.16.20.2.1.3.1.8.2
Global Chambersign Root - 2008	
Entidad de Certificación de la Administración Pública Andorrana (Andorra)	CPS Propia AnyPolicy
PERSONA FÍSICA en DSCF – SIGNATURA	2.16.20.2.1.3.1.1.3
PERSONA FÍSICA en DSCF – IDENTITAT	2.16.20.2.1.3.1.1.1
PERSONA FÍSICA en programari	2.16.20.2.1.3.1.1.2
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PERSONA FÍSICA PROFESSIONAL en programari	2.16.20.2.1.3.1.12.2
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	2.16.20.2.1.3.1.12.3
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	2.16.20.2.1.3.1.12.1
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1

PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	2.16.20.2.1.3.1.12.2
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.4.3
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.4.1
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en programari	2.16.20.2.1.3.1.4.2
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	2.16.20.2.1.3.1.5.3
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	2.16.20.2.1.3.1.5.1
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	2.16.20.2.1.3.1.11.1
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ en programari	2.16.20.2.1.3.1.5.2
SEGELL D'EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	2.16.20.2.1.3.1.2.3
SEGELL D'EMPRESA (Persona Jurídica) en HSM – IDENTITAT	2.16.20.2.1.3.1.2.1
SEGELL D'EMPRESA (Persona Jurídica) en programari	2.16.20.2.1.3.1.2.2
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	2.16.20.2.1.3.1.3.3
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	2.16.20.2.1.3.1.3.1
REPRESENTANT PERSONA JURÍDICA en programari	2.16.20.2.1.3.1.3.2
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en HSM	2.16.20.2.1.3.1.8.3
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en programari	2.16.20.2.1.3.1.8.2
AC Camerfirma - 2009	AnyPolicy
AC Camerfirma Portugal - 2015	AnyPolicy
MULTICERT SSL Certification Authority 001	CPS Propia AnyPolicy
GLOBAL CORPORATE SERVER	AnyPolicy

1.3.5.10.1 AC Camerfirma

Los certificados emitidos por esta AC tendrán continuidad con los mismos OID en la AC "AC Camerfirma – AAAA". Siendo AAAA el año de emisión del certificado

El objeto de esta AC intermedia será la de emitir certificados de AC sectoriales (Banca, Sanidad…etc.). En la actualidad solo se ha desarrollado Bajo esta AC intermedia una AC marca blanca de propósito general llamada RACER.

1.3.5.10.1.1 AC RACER (Red de Alta Capilaridad de Entidades de Registro)

Los certificados emitidos por esta AC tendrán continuidad con los mismos OID en la AC "RACER – AAAA". Siendo AAAA el año de emisión del certificado.

La principal característica de RACER es que puede utilizar cualquier agente como Autoridad de Registro siempre que previamente haya recibido la adecuada formación y haya sido objeto de un proceso de alta y de una auditoria que verifique que se encuentra en disposición de dar adecuado cumplimiento a las "obligaciones" estipuladas en las correspondientes Políticas de Certificación.

Bajo esta AC se permite solicitar certificados de persona física que no determinan la relación o vinculación de la persona física con una entidad jurídica y simplemente garantiza la identidad de la persona física como Firmante/ Suscriptor, titular del certificado.

Las políticas de RACER no definen un ámbito territorial concreto, por lo que puede emitir certificados en cualquier parte donde exista una AR reconocida que cumpla los requisitos establecidos por Camerfirma y *sujetándose en todo caso a la legislación vigente aplicable a las relaciones comerciales internacionales*. No obstante, el desarrollo de la Jerarquía Chambersign Global Root organiza la emisión de certificados digitales en diferentes países mediante el establecimiento de Autoridades de Certificación expresamente creadas para la emisión de certificados en un país concreto y permitiendo adaptarse así de mejor manera al marco jurídico y reglamentario concreto.

1.3.5.10.2 Entidad de Certificación de la Administración Pública Andorrana.

Siguiendo las pautas de organización de la jerarquía, se ha creado esta Autoridad de Certificación con objeto de emitir certificados en el ambito geográfico del Principado de Andorra. Se rige por su propia CPS.

De manera general, la jerarquía pública de certificación de Andorra incluye:

- La emisión de certificados en el sector público de Andorra y los ciudadanos de Andorra, entendiéndose como ciudadanos de Andorra las personas físicas o jurídicas de nacionalidad andorrana o con residencia legal en Andorra.
- La admisión de certificados de los ciudadanos andorranos y de los extranjeros no residentes en Andorra, en sus relaciones electrónicas con el sector público de Andorra.

A los efectos de este documento, por sector público debe entenderse:

- La Administración Pública, tal y como se define en el artículo 13 del Código de Administración:
- El Consejo Ejecutivo y los órganos puestos bajo su dirección.
- Los Comunes y Cuartos y los órganos que dependen.
- Los organismos autónomos o entidades parapúblicas.
- Las sociedades mercantiles públicas, participadas por la Administración Pública.

En función del uso de los certificados, se establece la siguiente clasificación de los certificados:

- Certificados de firma electrónica, que permiten su uso para la autenticación de documentos por parte de una persona física, de acuerdo con la definición contenida en el artículo 7 de la Ley 6 /2009, de 29 de diciembre, de firma electrónica. Los certificados pueden ser ordinarios o cualificados.

  Con carácter general, los certificados ordinarios cumplen los requisitos que se prevén en la especificación técnica ETSI TS 102 042, para la política NCP o NCP +, cuando se requieren superiores garantías de seguridad.

  Por su parte, los certificados calificados cumplen los requisitos que se prevén en la especificación técnica ETSI TS 101 456, para la política QCP público o QCP + SSCD, cuando se emiten conjuntamente con un dispositivo seguro de creación de firma electrónica.

- Certificados de sello electrónico, que permiten su uso para la autenticación de documentos por parte de una persona jurídica.

  Con carácter general, los certificados de sello electrónico cumplen los requisitos que se prevén en la especificación técnica ETSI TS 102 042, para la política NCP o NCP +, cuando se requieren superiores garantías de seguridad.

- Certificados de identidad electrónica, que permiten su uso para la identificación electrónica de una persona física o jurídica.

  Con carácter general, los certificados de identidad cumplen los requisitos que se prevén en la especificación técnica ETSI TS 102 042, para la política NCP o NCP +, cuando se requieren superiores garantías de seguridad.

- Certificados de cifrado, que permiten su uso para la garantía de la confidencialidad de los documentos y las transmisiones de datos.

  Con carácter general, los certificados de cifrado cumplen los requisitos que se prevén en la especificación técnica ETSI TS 102 042, para la política NCP.

En función del adquirente de los certificados, esta política establece la siguiente clasificación:

- Certificados corporativos públicos, adquiridos por parte del sector público para cubrir sus necesidades de seguridad.

- Certificados de la ciudadanía, emitidos por la Entidad de Certificación de la Administración Pública Andorrana, o por otros prestadores de servicios de certificación, cuando hayan sido objeto de admisión por parte de la Administración Pública.

Las características particulares de esta Autoridad de Certificación hacen necesaria la redacción de un documento independiente de las prácticas de certificación generales de AC Camerfirma SA. Estas prácticas están disponibles tanto en castellano como en catalán solicitándolas a a la propia Administración Pública Andorrana.

1.3.5.10.3 AC Camerfirma – 2009

Esta es una CA de infraestructura que solo emite otros certificados de CA que se rigen por sus propias CPS.

1.3.5.10.4 AC Camerfirma Portugal - 2015

Esta es una CA de infraestructura que solo emite otros certificados de CA en el ámbito territorial de Portugal o para entidades de nacionalidad portuguesa y que se rigen por sus propias CPS.

1.3.5.10.5 MULTICERT SSL Certification Authority 001

Se ha creado esa CA intermedia que pasa a ser propiedad de la entidad MULTICERT y que emite certificados de servidor seguro (SSL) exclusivamente y que se rige por sus propias CPS.

1.3.5.10.6 GLOBAL CORPORATE SERVER

Esta es una CA de infraestructura que solo emite otros certificados de CA propiedad de terceras entidades que emiten certificados de servidor seguro (SSL) exclusivamente y que se rigen por sus propias CPS

1.4. Ámbito de aplicación y usos

Esta CPS da respuesta a las Políticas de Certificación descritas en el apartado 1.2 de la presente CPS.

1.4.1 Usos apropiados de los certificados

Los certificados de Camerfirma podrán usarse en los términos establecidos por las Políticas de Certificación correspondientes y en su defecto, por lo establecido en este documento.

En términos generales, admiten los certificados para los siguientes usos:

- Autenticación basada en certificados X.509v3.
- Firma electrónica, avanzada o reconocida, basada en certificados X.509v3.
- Cifrado asimétrico o mixto, basado en certificados X.509v3.

1.4.2 Usos prohibidos de los certificados

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso y que vienen descritos en las políticas de certificación correspondientes.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

El empleo de los certificados digitales en operaciones que contravienen las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS o los Contratos de la AC con las AR o con sus Firmantes/Suscriptores tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

Camerfirma no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de Camerfirma emitir valoración alguna sobre dicho contenido, asumiendo por tanto el firmante cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado. Asimismo, le será imputable al firmante cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los contratos de la AC con sus Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

Camerfirma incorpora en el certificado información sobre la limitación de uso, bien en campos estandarizados en los atributos “uso de la clave” (*key usage*), “restricciones básicas” (*basic constrains*) y/o “restricciones de nombre” (*name constrains*) marcados como críticos en el

certificado y por lo tanto de cumplimiento obligatorio por parte de las aplicaciones que lo utilicen, o bien limitaciones en atributos como "uso extendido de clave" (*extended key usage*) y/o mediante textos incorporados el campo "declaración del emisor" (*user notice*) marcados cono "no crítico" pero de obligado cumplimiento por parte del titular y del usuario del certificado.

1.5. Autoridad de Políticas

Esta CPS define la forma en que la Autoridad de Certificación da respuesta a todos los requerimientos y niveles de seguridad impuestos por las Políticas de Certificación correspondientes.

La actividad de la Autoridad de Certificación podrá ser sometida a la inspección de la Autoridad de las Políticas (PA) o por personal delegado por la misma.

Para las jerarquías descritas en este documento la autoridad de las Políticas corresponde al departamento jurídico de Camerfirma.

1.5.1 Organización que administra el documento

La redacción y control de esta CPS está gestionada por el departamento jurídico de AC Camerfirma SA con la colaboración del departamento de explotación.

1.5.2 Datos de contacto de la organización

Dirección:	Calle Ribera del Loira, 12. Madrid (Madrid)
Teléfono:	902 361 207
Fax:	902 930 422
Email:	juridico@camerfirma.com

En lo que se refiere al contenido de esta CPS, 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 puede informarse a este respecto en la Web de Camerfirma http://www.camerfirma.com donde puede encontrar información general sobre el uso de la firma digital y los certificados digitales.

Para reportar incidentes de seguridad relacionados con los certificados por el TSP pueden ponerse en contacto con AC Camerfirma mediante a través de una comunicación dirigida a la cuenta de email incidentes@camerfirma.com

1.5.3 Persona que determina la idoneidad de CPS para la política

El departamento jurídico de Camerfirma se constituye por lo tanto en la Autoridad de las Políticas (PA) de las Jerarquías y Autoridades de Certificación descritas anteriormente siendo responsable de la administración de la CPS.

1.5.4 Procedimientos de gestión del documento

La publicación de las revisiones de esta CPS deberá estar aprobada por la Gerencia de Camerfirma.

AC Camerfirma publica en su página web cada nueva versión. LA CPS está publicada en formato PDF firmado electrónicamente con el certificado digital de los responsables de los departamos Juridico y de Explotación de AC Camerfirma SA.

1.6. Acrónimos y Definiciones.

1.6.1 Acrónimos

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

1.6.2 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 Sujeto/Firmante y la Parte Usuaria, 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 Sujeto/Firmante 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 Sujeto/Firmante 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
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 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 Sujeto/Firmante 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 Sujeto/Firmante 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 Sujeto/Firmante.
Entidad	Dentro del contexto de estas políticas de certificación, aquella empresa u organización de cualquier tipo con la que el solicitante tiene algún tipo de vinculación.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.

Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes
Solicitante	Dentro del contexto de esta política de certificación, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de la entidad.
Sujeto/Firmante	Dentro del contexto de esta declaración de prácticas de certificación, la persona física cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Parte Usuaria	Dentro del contexto de esta política de certificación, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado

2. RESPONSABILIDAD DE PUBLICACIÓN Y REPOSITORIOS

2.1. Repositorios

Camerfirma dispone de un servicio de consulta de certificados emitidos y listas de revocación. Estos servicios están disponibles públicamente en su página Web: https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Los servicios de consulta están diseñados para garantizar una disponibilidad de 24 horas por día 7 días a la semana.

Repositorio de políticas y prácticas de certificación. Esta información está disponible públicamente en la página web de Camerfirma https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/.

Camerfirma publica los certificados emitidos, las listas de revocación, políticas y prácticas de certificación de forma libre y gratuita en https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

Camerfirma solicita previamente la autorización del titular antes de proceder a la publicación del certificado.

2.2. Publicación de información de certificados

De manera general Camerfirma publica las siguientes informaciones en su repositorio:

- Un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida, o extinguida.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La política general de certificación y, cuando sea conveniente, las políticas específicas.
- Los perfiles de los certificados y de las listas de revocación de los certificados.
- La Declaración de Prácticas de Certificación.
- Los instrumentos jurídicos vinculantes con suscriptores y verificadores.

Todo cambio en las especificaciones o condiciones del servicio será comunicado a los usuarios por la Entidad de Certificación, a través de su página web http://www.camerfirma.com

No se retirará la versión anterior del documento objeto del cambio, se indicará que ha sido sustituido por la versión nueva.

La publicación de certificados por SubCA externas se realizan en un repositorio proporcionado por AC Camerfirma, o en su caso, en un repositorio propio al cual, por acuerdo contractual, Camerfirma pueda tener acceso.

2.2.1 Políticas y Prácticas de Certificación.

La presente CPS y Políticas actuales están disponibles públicamente en el sitio de Internet: https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

Las políticas de certificación de AC subordinadas también estarán publicadas o referenciadas en el sitio internet de AC Camerfirma. https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

2.2.2 Términos y condiciones.

Camerfirma pone a disposición de los usuarios, los términos y condiciones del servicio, en sus políticas y prácticas de certificación. El Sujeto/Firmante recibe información de los términos y condiciones en el proceso de emisión del certificado, bien mediante la forma del contrato físico o bien mediante el proceso de aceptación por vía electrónica de condiciones del servicio como paso indispensable para proceder a la solicitud.

Cuando el sujeto/firmante acepta los términos y condiciones en papel debe hacerse a través de una firma manuscrita. En el caso de que se acepte en formato electrónico se realiza mediante la aceptación de condiciones y usos en el formulario de solicitud, de acuerdo con lo estipulado por la normativa vigente en materia de contratación por vía electrónica.

2.2.3 Difusión de los certificados.

Se podrá acceder a los certificados emitidos, siempre *que el Firmante/Suscriptor de su consentimiento*. El solicitante previo a la emisión del certificado, realiza una aceptación de usos, otorgando a Camerfirma la facultad de publicar el certificado emitido en el sitio Internet:

http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

Las claves raíz de las jerarquías Camerfirma se pueden descargar desde la dirección:
https://www.camerfirma.com/clavespublicas

El proceso de consulta de certificados se realiza desde una página Web en modo seguro, introduciendo el email del suscriptor. La respuesta del sistema, si encuentra un suscriptor con ese email, es una página con todos los certificados asociados ya estén activos, caducados, o revocados. De esta forma la consulta no es libre ni se pueden descargar certificados de forma masiva.

2.3. Frecuencia de publicación.

AC Camerfirma publica los certificados de entidad final inmediatamente después de haber sido emitidos y siempre tras la aprobación del Firmante/Suscriptor.

AC Camerfirma emite y publica listas de revocados de forma periódica siguiendo la tabla marcada en el apartado de estas prácticas *"Frecuencia de emisión de CRLs"*.

Camerfirma publica de forma inmediata en su página Web https://policy.camerfirma.com. Cualquier modificación en las Políticas y la CPS, manteniendo un histórico de versiones.

La información de Camerfirma se publicará cuando se encuentre disponible y en especial, de forma inmediata cuando se emitan las menciones relativas a la vigencia de los certificados.

Los cambios en la CPS se regirán por lo establecido en la sección correspondiente de la CPS.

La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en la sección correspondiente de esta CPS.

Al cabo de 15 (quince) días desde la publicación de la nueva versión, se podrá retirar la referencia al cambio de la página principal y se inserta en el depósito. Las versiones antiguas de la documentación serán conservadas, por un periodo de 15 (quince) años por la Entidad de Certificación, pudiendo ser consultadas, por causa razonada por los interesados.

2.4. Controles de acceso a los repositorios.

Camerfirma publica los certificados y CRL en su página web. Para el acceso al directorio de certificados se necesitará el email del titular y pasar un control anti-robot, eliminando así la posibilidad de búsquedas y descargas masivas.

El acceso a la información de revocación así como a los certificados emitidos por Camerfirma es libre y gratuito.

Camerfirma utiliza sistemas fiables para el repositorio, de tal manera que:

- Se pueda comprobar la autenticidad de los certificados. El propio certificado mediante la firma por la autoridad de certificación garantiza su autenticidad.
- Las personas no autorizadas no puedan alterar los datos. La firma electrónica de la autoridad de certificación protege de la manipulación de los datos incluidos en el certificado.
- Los certificados sólo sean accesibles en los supuestos a las personas que el firmante haya indicado. El solicitante autoriza o no a la publicación de su certificado en el proceso de solicitud.
- Se pueda detectar cualquier cambio técnico que afecte a los requisitos de seguridad. La base de datos que sirve de repositorio posee mecanismos de protección en integridad y acceso no autorizado. Identificación y Autenticación

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Denominación

3.1.1 Tipos de nombres

El Firmantes/Suscriptor se describe en los certificados mediante un nombre distintivo (DN, distinguished name, Subject) conforme al estándar X.501. Las descripciones del campo DN están reflejadas en cada una de las fichas de perfil de los certificados. Asimismo, incluye un componente " Common Name "(CN =).

Las fichas de perfil se pueden solicitar a través del servicio de soporte a cliente de AC Camerfirma 902 361 207 o a través del aplicativo.https://www.camerfirma.com/ayuda/soporte/

La estructura sintáctica y el contenido de los campos de cada certificado emitido por Camerfirma así como su significado semántico se encuentran descritos en cada una de las fichas de perfil de los certificados.

- Personas físicas: En certificados correspondientes a personas físicas la identificación del signatario estará formada por su nombre y apellidos, más su identificador fiscal.
- Personas Jurídicas (Sellos): En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su identificación fiscal.
- La estructura para los certificados de AC subordinada, OCSP, incluye como mínimo:
    - Un nombre descriptivo que identifica a la Autoridad de Certificación (CN)
    - La persona jurídica responsable de las claves (O)
    - El identificador fiscal de la organización responsable de las claves (*OrganizationIdentifier*)
    - El país donde realiza la actividad la empresa responsable de las claves. (C)
- Los certificados de *ROOT* tienen un nombre descriptivo que identifica a la Autoridad de Certificación y en el campo (O) el nombre la organización responsable de la Autoridad de Certificación

3.1.2 Significado de los nombres

Todos los Nombres Distinguidos deben ser significativos, y la identificación de los atributos asociados al suscriptor debe ser en una forma legible por humanos. Ver 7.1.4

3.1.3 Anonimato o pseudónimos de suscriptores

No aplicable.

3.1.4 Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.5 Unicidad de los nombres

Dentro de una misma AC no se puede volver a asignar un nombre de suscriptor que ya haya sido ocupado, a un suscriptor diferente, esto se consigue incorporando el identificador fiscal único a la cadena del nombre que distingue al titular del certificado.

3.1.5.1 Emisión de varios certificados de persona física para un mismo titular

Bajo esta CPS un Firmante persona física puede pedir más de un certificado siempre que la combinación de los siguientes valores en la solicitud sea diferente:

- CIF
- DNI-Tarjeta de residente.
- Tipo de certificado: Identificador de política.
- Soporte (Software, tarjeta)

También puede considerarse un certificado diferente cuando la posición, atributo título (title) o departamento, en el campo titular del certificado sea diferente.

3.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos

Camerfirma no asume compromisos en la emisión de certificados respecto al uso de marcas y otros signos distintivos. Camerfirma no permite deliberadamente el uso de un signo distintivo sobre el Sujeto/Firmante que no ostente derechos de uso. Sin embargo, Camerfirma no está obligada a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados, por lo que puede negarse a generar o solicitar la revocación de cualquier certificado involucrado en una disputa.

3.1.7 Procedimiento de resolución de disputas de nombres

Camerfirma no tiene responsabilidad en el caso de resolución de disputas de nombres. En todo caso, la asignación de nombres se realizará basándose en su orden de entrada.

Camerfirma no arbitra este tipo de disputas que deberán ser resueltas directamente por las partes.

3.2. Validación inicial de la identidad

La comprobación de la identidad no diferencia entre certificados de distintas jerarquías sino que está asociada al tipo de certificado emitido.

Para realizar una correcta identificación de la identidad del Solicitante, de la entidad y de su vinculación, Camerfirma a través de la AR, exige:

3.2.1 Métodos de prueba de la posesión de la clave privada.

Camerfirma emplea diversos circuitos para la emisión de certificados donde la clave privada se gestiona de diferente forma. La clave privada puede ser generada tanto por el usuario como por Camerfirma.

a) Generación de claves por parte de Camerfirma.

   En Software: Se entregan al Sujeto/Firmante en mano o mediante correo a través de ficheros protegidos utilizando el Standard PKCS#12. La seguridad del proceso queda garantizada debido a que el código de acceso al fichero PKCS#12 que posibilita la instalación de éste en las aplicaciones, es entregada por un medio distinto al utilizado en la recepción del fichero.

   En Hardware: Las claves pueden ser entregadas por Camerfirma al Sujeto/Firmante, directamente o a través de una autoridad de registro en un dispositivo cualificado de creación de firma (QSCD).

   En almacenamiento remoto centralizado: Camerfirma utiliza un sistema de almacenamiento de claves remoto, permitiendo al Sujeto/Firmante acceder a la clave desde distintos dispositivos. Las claves se almacenan en un dispositivo HSM certificado FIPS-140-2 nivel 3 (incluido en la lista de dispositivos notificados por los estados miembros como dispositivos cualificados seguros de creación de firma https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds) asegurando el control único de dicha clave por parte del Sujeto/Firmante. Este tipo de almacenamiento no se realiza para los certificados de servidor seguro SSL/TLS

b) Generación de las claves por el suscriptor.

   El Firmante dispone de un mecanismo de generación de claves ya sea software o hardware, La prueba de posesión de la clave privada en estos casos es la petición recibida por Camerfirma en formato PKCS#10 o criptográficamente equivalente.

3.2.2 Identificación de la entidad

3.2.2.1 Identidad

Con carácter previo a la emisión y entrega de un certificado emitido a una persona jurídica (certificado de sello electrónico) o a una persona física con atributo de vinculación a una entidad, es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad.

Para estos certificados, se exige en todos los casos, la identificación de la entidad, para lo que la RA requerirá la documentación pertinente en función del tipo de entidad. La documentación pertinente se encuentra en la web de Camerfirma en el apartado informativo del certificado correspondiente.

En el caso de entidades fuera del territorio español, la documentación que deben aportar será la del Registro Oficial del país correspondiente debidamente apostillada y con traducción jurada en idioma español donde se indique la existencia de la entidad en dicho país.

Además, se comprueba:

- Que los datos o documentos aportados no tengan una antigüedad superior a 1 año.
- Que la antigüedad de existencia legal de la organización es de 1 año mínimo.
- Que no se trata de empresas erradicadas en países donde exista una prohibición gubernamental para hacer negocios o formen parte de alguna lista negra de entidades gestionada por el prestador.

En Administraciones públicas: No se exige la documentación acreditativa de la existencia de la administración pública, organismo o entidad de derecho público, dado que dicha identidad forma parte del ámbito corporativo de la Administración General del Estado o de otras AAPP del Estado.

3.2.2.2 Marcas registradas

Ver punto 3.1.6

3.2.2.3 Verificación del país

Ver punto 3.2.2.1

3.2.2.4 Validación de la autorización o control de dominio

Ver punto 3.2.5.1

3.2.2.5 Autenticación de una dirección IP

No aplicable.

3.2.2.6 Validación del dominio Wildcard

No aplicable.

3.2.2.7 Exactitud de las fuentes de datos

Ver punto 3.2.2.1

3.2.2.8 Registros CAA

No aplicable.

3.2.3 Identificación de la identidad de un individuo.

Con carácter previo a la emisión y entrega de un certificado, se exige la personación física del Sujeto/Titular o Firmante cuando éste sea una persona física o del Solicitante cuando el Sujeto/Titular es una entidad jurídica, presentando alguno de los siguientes documentos:

- Documento Nacional de Identidad.
- Tarjeta de residencia.
- Pasaporte o documento de identidad del país del Sujeto/Titular
- Documento de identidad apostillado para solicitantes fuera del territorio español

La presencia física no es obligatoria en estos certificados en los casos que marca la ley 59/2003 y las normas de ámbito europeo directamente aplicables en España.

En el caso de documentos de identidad extranjeros, se podrá pedir traducción jurada en castellano con apostilla de la Haya si se considera necesario.

Se comprueba el control sobre la dirección de correo electrónico incorporada en la solicitud de certificado mediante la comunicación de un valor aleatorio que será requerido en el momento de la generación y descarga del certificado.

3.2.4 Información de suscriptor no verificada

No está permitido bajo estas prácticas de certificación incluir información no verificada en el "subject" de un certificado.

3.2.5 Validación de la autoridad

3.2.5.1 Identificación de la vinculación.

Tipo de certificado	Documentación
Certificado de representante (AC Camerfirma Certificados Camerales) Certificado de apoderado (AC Camerfirma Certificados Camerales) Certificado de representante de Persona Jurídica (o de Entidad sin Personalidad Jurídica) para trámites con las AAPP *(hasta el 8 de junio de 2020)* Certificado de Persona Física de Vinculación Representación (RACER) Certificado de Persona Física de Vinculación Apoderado (RACER)	Evidencia sobre la capacidad de representación del Sujeto/Firmante respecto de la entidad, mediante la entrega de la documentación que demuestre sus facultades de representación en función del tipo de entidad. Esta información se publica en los Manuales operativos de la RA y en la página web de Camerfirma.
Certificado de pertenencia a empresa (AC Camerfirma Certificados Camerales) Certificado de Cifrado (Software) (AC Camerfirma Certificados Camerales) Certificado de Factura electrónica (AC Camerfirma Certificados Camerales) Certificado de Persona Física de Vinculación Pertenencia (RACER)	En general, autorización firmada por un representante legal o apoderado general de la entidad que acredita la vinculación del Solicitante con la Entidad

Tipo de certificado	Documentación
Certificado de Persona Física Ciudadano Emprendedor (RACER) Certificado de Persona Física de Vinculación Factura Electrónica (RACER)	
Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho publico, nivel alto (AC CAMERFIRMA AAPP) Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho publico, nivel medio (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel alto, firma (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel alto, autenticación (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel alto, cifrado (AC CAMERFIRMA AAPP) Certificado reconocido de empleado publico, nivel medio (AC CAMERFIRMA AAPP)	Documento de identidad de la persona que actúa como responsable, en nombre de dicha Administración Pública, organismo o entidad de derecho público. El Solicitante/responsable se identificará ante la RA con su DNI y autorización de la persona responsable donde se indique que es empleado público o nombramiento en Boletín Oficial donde conste el NIF de esta persona. Documento acreditativo que evidencie la titularidad del dominio usado en el correo del solicitante por parte de la entidad asociada al certificado de sello electrónico. Los documentos admitidos pueden ser: facturas o contrato de compra.

Tipo de certificado	Documentación
Certificat d´actuació de PERSONA FÍSICA al servei de l´ADMINISTRACIÓ (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de PERSONA FÍSICA (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de PERSONA FÍSICA al servei d'una ORGANITZACIÓ (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL COL·LEGIAT (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació de REPRESENTANT PERSONA JURÍDICA (Entidad de Certificación de la Administración Pública Andorrana + RACER)	El artículo 26.2 de la Ley Andorrana 35/2014, de 27 de noviembre, de servicios fiduciarios electrónicos, establece que: "el prestador de servicios de confianza electrónico cualificado deberá verificar fehacientemente la identidad y, en su caso, cualquier otra atribución específica de la persona natural a quien le expide el certificado electrónico cualificado, mediante la exhibición de los documentos públicos o privados que acredite suficientemente. Esta información debe ser verificada por el proveedor de servicios cualificado o por un tercero que actúe bajo la responsabilidad del proveedor de servicios cualificado: i. A través de la presencia física de esta persona, o ii. A distancia, utilizando otros certificados electrónicos reconocidos emitidos por un proveedor de servicios cualificado". Por otra parte, el artículo 26.3 de la Ley Andorrana 35/2014, de 27 de noviembre, de servicios de confianza electrónico, establece que en el caso de: "certificados electrónicos expedidos a personas físicas pero vinculadas a una organización, entidad, institución, empresa u otra persona jurídica, el prestador del servicio de confianza deberá acreditar, además de la identidad del solicitante y de la persona identificada en el certificado electrónico, los datos relativos a la constitución y personalidad jurídica de la entidad, o a la extensión y validez de las facultades o poderes de representación del solicitante, mediante los documentos públicos que acredite de forma específica o mediante la consulta del registro público correspondiente, que es el resultado de los datos que deban figurar en el mismo".
Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica) (Entidad de Certificación de la Administración Pública Andorrana + RACER) Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic (Entidad de Certificación de la Administración Pública Andorrana + RACER)	El artículo 26.2 de la Ley Andorrana 35/2014, de 27 de noviembre, de servicios fiduciarios electrónicos, establece que: "el prestador de servicios de confianza electrónico cualificado verificará la identidad y, en su caso, cualquier otra atribución específica de la persona jurídica a la que se expida el certificado electrónico cualificado, mediante la exhibición de documentos públicos o privados que acredite suficientemente. Esta información debe ser verificada por el proveedor de servicios cualificado o por un tercero que actúe bajo la responsabilidad del proveedor de servicios cualificado: i. Mediante la presencia física de un representante autorizado de dicha persona jurídica, o ii. A distancia, utilizando otros certificados electrónicos reconocidos emitidos por un proveedor de servicios cualificado".

3.2.5.2 Consideraciones en la identificación de usuario en casos de alto cargo.

AC Camerfirma emplea procedimientos especiales para la identificación de altos cargos en empresas y administración para la emisión de certificados digitales. En estos casos un operador

de registro se desplaza a las instalaciones de la organización para garantizar la presencia física del titular. Para las relaciones entre el titular y la organización representada en administración pública se suele usar la publicación de los cargos en los boletines oficiales.

3.2.5.3 Consideraciones en la identificación de usuarios y vinculación en el AAPP

Existen aspectos a considerar respecto a las Autoridades de Registro establecidas en la administración pública y operadas por empleados públicos, teniendo estos últimos consideración de fedatarios publicos para garantizar la relación entre un empleado público que solicita el certificado y el organismo al que está vinculado. En estos casos se puede simplificar la recogida de documentación que forma parte del expediente.

3.2.5.4 En los certificados de operador de RA.

Se comprueba por un lado que el solicitante ha superado el examen de operador y por otro lado que los datos son idénticos a los de la ficha de operador de RA entregada por la organización a la cual pertenece el operador. Se comprueba que el CIF se asocia a la organización y que el mail asociado al certificado es un mail de la organización.

3.2.5.5 Consideraciones especiales para la emisión de certificados fuera del territorio español.

Aspectos que tiene que ver con la documentación de identidad de las personas físicas, jurídicas y vinculaciones entre ellas en los diferentes países donde Camerfirma emite certificados. La documentación requerida para ello es la que legalmente procede en cada país siempre y cuando permita cumplir con la obligación de identificación correspondiente de acuerdo con la legislación española.

3.2.6 Criterios para la interoperación

Camerfirma puede proporcionar servicios que permitan que otra CA opere dentro de, o interopere con, su PKI. Dicha interoperación puede incluir certificación cruzada, certificación unilateral u otras formas de operación. Camerfirma se reserva el derecho de proporcionar servicios de interoperación e interoperar con otras CA; los términos y criterios de los cuales deben establecerse contractualmente.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados

La identificación de una solicitud de renovación se realiza a través del certificado a renovar. No se renovará si el certificado para renovar ha pasado los 5 años desde la última verificación física o proceso equivalente.

3.3.2 Identificación y autenticación de la solicitud de renovación tras una revocación

La política de identificación y autenticación para la renovación del certificado después de una revocación será la misma que para el registro inicial.

Excepción: Cuando la revocación se produce en certificados de entidad final como consecuencia de un proceso de sustitución del certificado o por un error en su emisión o una pérdida, se considera que la renovación después de una revocación puede realizarse, siempre que este refleje la situación actual. Se reutilizará la documentación soporte entregada para la emisión del certificado sustituido y se eliminaría la personación física, si esta fuera requerida por la naturaleza del certificado. Camerfirma actualizará el número de años desde la última personación física al estado que tuviera el certificado a sustituir, de la misma forma que si este proceso hubiera sido consecuencia de una renovación ordinaria.

3.4. Identificación y autenticación de la solicitud de revocación

La forma de realizar las solicitudes de revocación se establece en el apartado 4.9.3 de este documento.

Camerfirma, o cualquiera de las entidades que lo componen, puede, por propia iniciativa, solicitar la revocación de un certificado si conoce o sospecha que la clave privada del suscriptor se ha visto comprometida, o si conoce o sospecha de cualquier otro evento que aconseje tomar dicha medida.

4. REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

AC Camerfirma emplea para la gestión del ciclo de vida de los certificados su plataforma STATUS. Esta plataforma permite la solicitud, registro, publicación, revocación de todos los certificados emitidos.

4.1. Solicitud de certificados

4.1.1 Quién puede realizar la solicitud de un certificado

Una solicitud de certificado puede ser presentada por el sujeto del certificado o por un representante autorizado del mismo.

4.1.2 Procedimiento de alta y responsabilidades

4.1.2.1 Formularios Web.

Las solicitudes de los certificados se realizan de forma general mediante el acceso a los formularios de solicitud en la dirección, o mediante el envío al solicitante de un enlace a un formulario concreto.

http://www.camerfirma.com/certificados/

En la página Web se encuentran los formularios necesarios para realizar la solicitud de cada tipo de certificado distribuido por Camerfirma en diferentes formatos y los dispositivos de generación de firma, si estos fueran necesarios.

El formulario permitirá la incorporación de un CSR (PKCS#11) en caso de que el usuario haya creado las claves.

El usuario recibe, posteriormente a la confirmación de los datos de solicitud, un correo electrónico en la cuenta asociada a la solicitud del certificado un enlace para confirmar la solicitud y aceptar las condiciones de uso.

Una vez confirmada la solicitud el suscriptor es informado de la documentación que debe presentar en una oficina de registro habilitada y cumplir con el requisito de identificación presencial si esta es pertinente.

4.1.2.2 Lotes.

La plataforma STATUS permite igualmente circuitos de solicitud mediante lotes. En este caso, se enviará por el solicitante a la AR un fichero estructurado según un diseño prefijado por Camerfirma con los datos de los solicitantes. La AR procederá a la carga de dichas peticiones en el aplicativo de gestión.

4.1.2.3 Solicitudes de certificados de entidad final en HSM.

Las solicitudes para la emisión de certificados en HSM se realizarán mediante una petición de oferta comercial a través de un comercial de zona. http://www.camerfirma.com/camerfirma/localizacion.

AC Camerfirma se reserva el derecho a enviar un auditor interno o externo para comprobar que el desarrollo de la ceremonia de creación de claves se ajusta a las políticas de certificación y practicas correspondientes.

Cuando el cliente genere por sus propios medios las claves criptográficas en un dispositivo HSM y solicite un certificado en hardware, Camerfirma recopilará las evidencias necesarias, para lo cual solicitará la siguiente documentación:

- Declaración responsable del solicitante indicando que las claves han sido generadas dentro de un dispositivo hardware y/o un informe técnico de un tercero (proveedor de servicios) que certifique dicho proceso. AC Camerfirma dispondrá de modelos de declaración para los suscriptores y terceros.

- Acta de ceremonia de creación de las claves indicando:

    - El proceso seguido para la creación de las claves
    - Las personas implicadas
    - El entorno en el que se ha realizado
    - El equipo HSM utilizado (modelo y marca)
    - Políticas de seguridad empleadas : (tamaño de claves, parámetros de creación de la clave, exportable/no exportable y cualquier dato relevante adicional)
    - La solicitud PKCS#10 generada
    - Incidencias presentadas y su resolución.

- Características del dispositivo: Puede valer una ficha técnica del dispositivo

Esta información se incorporará por parte de la AR al expediente documental soporte para la emisión del certificado.

4.1.2.4 Solicitudes vía capa de Web Services (WS).

Con objeto de incorporar la integración de aplicaciones de terceros con la plataforma de gestión de certificados de Camerfirma (STATUS), se ha desarrollado una capa de Servicios Web (WS) que ofrecen procesos de emisión y revocación de certificados. Las llamadas a estos WS están firmadas con un certificado reconocido por la plataforma.

La emisión automáticade este tipo de certificados hace que el proceso sea revisado en detalle. Antes de iniciar la emisión mediante este sistema se debe contar con un informe técnico favorable de Camerfirma, un contrato donde la autoridad de registro se compromete a mantener el sistema en condiciones de seguridad óptimas y a notificar a Camerfirma cualquier modificación o incidencia. Adicionalmente el sistema deberá ser sometido a auditorias anuales donde se comprueba:

1. Expedientes documentales de los certificados emitidos

2. Que los certificados están siendo emitidos bajo las directrices marcadas por las políticas de certificación bajo la que se rigen.

4.1.2.5 Petición de certificación cruzada

Camerfirma permite bajo estas prácticas la certificación cruzada.

Camerfirma evaluará la solicitud y reclamará la entrega de las auditorias correspondientes que permitan certificar que el sistema vinculado cumple normativas técnicas, operativas y legales equiparables previamente a la generación del certificado.

Camerfirma solicita al cliente revisiones de auditorías anuales para mantener la certificación cruzada.

4.2. Procesamiento de las solicitudes de certificados

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez haya tenido lugar una petición de certificado, el operador de la RA mediante el acceso a la plataforma de gestión (STATUS) verifica la información proporcionada es conforme.

El operador de la plataforma posee un certificado de gestión interna emitido para realizar estas operaciones y que se obtiene después de un proceso de formación y evaluación.

El certificado utilizado por el operador de registro es considerado un acceso multi-factor usado no solo para el acceso a la plataforma de gestión PKI (STATUS) sino para aprobar cada petición de emisión de un certificado realizando una firma electrónica.

Cuando la solicitud de emisión sea para un certificado de servidor seguro o de sede electrónica la plataforma PKI examinará el registro CAA del DNS del dominio a certificar. Camerfirma denegará la certificación si en este registro se encuentra ocupado por una autoridad de certificación distinta según la RFC 6844. El cliente deberá modificar los datos de su dominio para permitir a Camerfirma emitirle dicho certificado.

Camerfirma usa la siguiente etiqueta en el registro CAA: “issue” o “issuewild” para poder emitir un certificado: “camerfirma.com”

4.2.2 Aprobación o rechazo de la solicitud

Para los certificados de entidad final:

El operador de registro visualiza las peticiones pendientes de tramitar y que le han sido asignadas.

El operador de la RA queda a la espera de que el sujeto/Firmante entregue la documentación correspondiente.

En las solicitudes vía capa de WS la petición viene autenticada en origen aprobándose la emisión del certificado por parte de la plataforma cuando el origen y la autenticación es correcta.

Si la información no es correcta, el RA deniega la petición. En caso de que los datos se verifiquen correctamente la Entidad de Registro aprobará la emisión del certificado mediante la firma electrónica con su certificado de operador.

Para certificados de SubCA:

Mediante aceptación comercial correspondiente a la solicitud de un cliente.

4.2.3 Plazo para resolver la solicitud

Las solicitudes vía servicios web se ejecutan directamente al recibirse estas autenticadas con un certificado previamente reconocido por Camerfirma.

Las solicitudes presentadas por la plataforma PKI STATUS se validan una vez comprobada la documentación acreditativa asociado al perfil del certificado. Camerfirma procederá siempre que sea viable a eliminar las solicitudes mayores de 1 año.

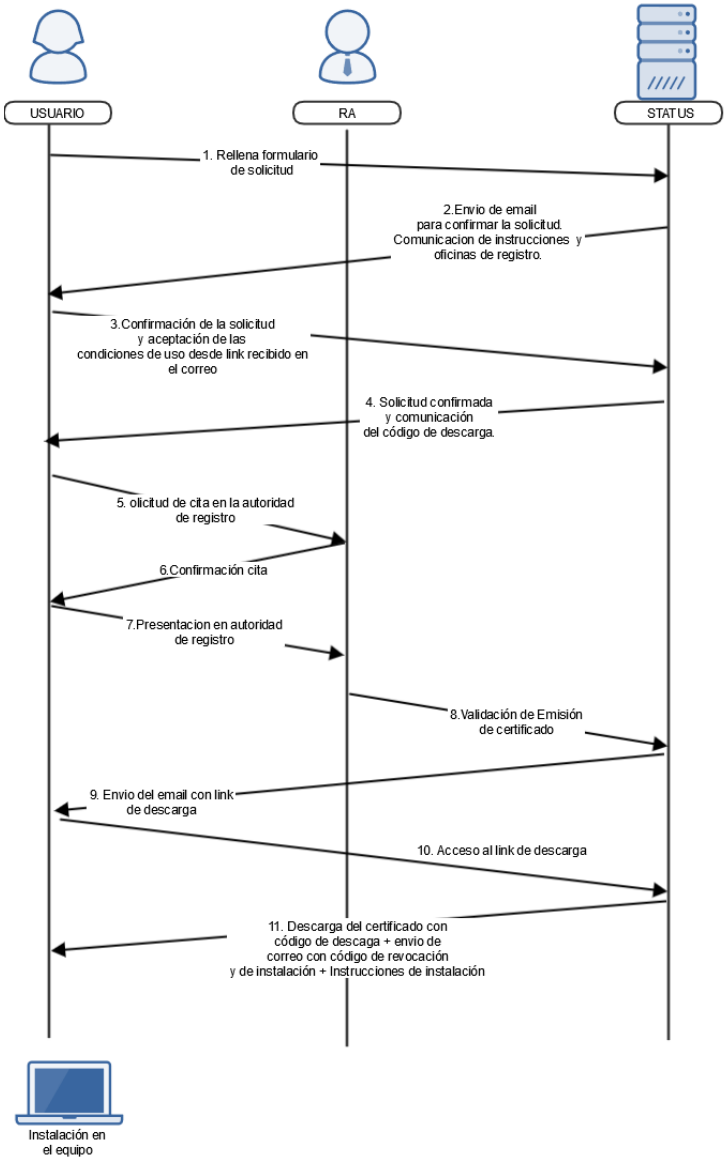
No existen plazos estipulados para resolver una solicitud de certificado de SubCA o certificación cruzada.

4.3. Emisión de certificados

4.3.1 Acciones de la CA durante el proceso de emisión

4.3.1.1 Certificados en Software

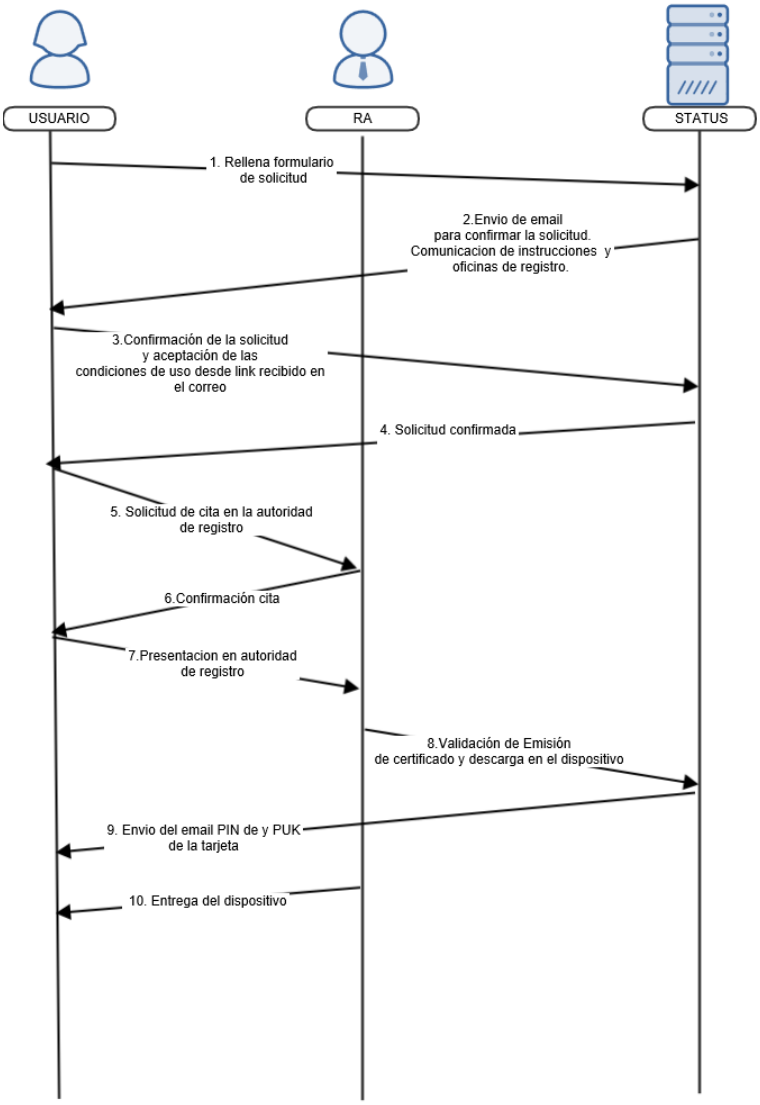
Una vez aprobada la solicitud el suscriptor recibe un correo electrónico con la notificación de este hecho y con él proceder a la generación y descarga del certificado. Para su instalación necesitara del código de producto que le ha sido entregado con el contrato y un código de instalación que se habrá entregado en un email independiente conjuntamente con un código de revocación.



Documento de referencia: IN-2008-03-01-Generacion_certs_software

4.3.1.2 Certificados en HW (Dispositivo Seguro de Creación de Firma):

4.3.1.2.1 Certificados en HW (Dispositivo Seguro de Creación de Firma): En Tarjeta o Token Criptográfico



Documento de referencia: IN-2008-03-02-Generacion_certs_tarjeta_tecnico

El usuario recibe en las dependencias de la AR el dispositivo de firma con los certificados y las claves generadas.

El operador de la Autoridad de Registro elegirá sobre qué tipo de tarjeta criptográfica quiere realizar la generación de las claves, para lo cual la estación de trabajo del operador de la autoridad de registro estará configurada adecuadamente con el CSP (*Criptographyc Service Provider*) correspondiente. Actualmente AC Camefirma admite varios tipos de tarjetas y tokens USB todos ellos certificados CWA 14169 SSCD Type-3.

Para las tarjetas por defecto (distribuidas por Bit4id) el suscriptor recibirá en la cuenta de correo asociada, el código de acceso al dispositivo criptográfico y el código de desbloqueo, así como

una clave de revocación. Para el resto de las tarjetas la gestión de PIN/PUK está fuera del alcance de este documento.

4.3.1.3 Certificados emitidos mediante acceso WEBSERVICE

Las solicitudes pueden ser recibidas mediante llamadas convenientemente autenticadas desde los servicios WS de la aplicación STATUS según apartado 4.1.4.

4.3.2 Notificación de la emisión al suscriptor

Camerfirma notifica mediante un correo electrónico al solicitante la aprobación o denegación de la solicitud.

4.4. Aceptación de certificados

4.4.1 Conducta que constituye aceptación del certificado

Una vez entregado o descargado el certificado, el usuario dispone de un periodo de 7 días para comprobar su correcta emisión.

Si el certificado no ha sido emitido correctamente por causas técnicas, el certificado se revocará y se emitirá uno nuevo.

4.4.2 Publicación del certificado por la AC

AC Camerfirma ofrece un sistema de consulta del estado de los certificados emitidos, en su página web http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/. El acceso a esta página es libre y gratuito.

En algunos casos es requisito del supervisor nacional enviar los certificados y CRL emitidos por el prestador de forma periódica.

En el caso de certificados SSL EV se envía previamente a la emisión del certificado una notificación a diferentes servicios de registro acreditados. Este requisito es de obligado cumplimiento para el reconocimiento de los certificados SSL EV por Google en un proceso llamado “Certificate Transparency”.

4.4.3 Notificación de emisión de certificado por la CA a otras entidades

AC Camerfirma ofrece un sistema de consulta del estado de los certificados emitidos, en su página web https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/. El acceso a esta página es libre y gratuito.

En el caso de certificados SSL/TLS como parte del proceso de certificación trasparente (https://www.certificate-transparency.org) se envía previamente a la emisión final, un pre-certificado a un servicio de registro centralizados**.**

4.5. Uso del par de claves y los certificados

4.5.1 Uso del certificado y la clave privada del suscriptor

La limitación de uso de la clave viene definida en el contenido del certificado en las extensiones: *keyUsage*, *extendedKeyUsage* y *basicConstraints*

CA	Key Usage	Extended Key Usage	Basic Constraints
Chambers of Commerce Root	critical, cRLSign, keyCertSign	-	critical,CA:true
AC Camerfirma Certificados Camerales	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado de pertenencia a empresa	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de representante	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de representante para trámites con las AAPP (hasta el 8 de junio de 2020)	critical, digitalSignature, contentCommitment, keyEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado de apoderado	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Cifrado (Software)	critical, digitalSignature, contentCommitment, keyEncipherment	-	critical,CA:false
Certificado de Factura electrónica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
AC CAMERFIRMA AAPP	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado reconocido de sello electronico de Administracion, organo o entidad de derecho publico, nivel alto	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de sello electronico de Administracion, organo o entidad de derecho publico, nivel medio	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de empleado publico, nivel alto, firma	critical, nonRepudiation	-	critical,CA:false
Certificado reconocido de empleado publico, nivel alto, autenticacion.	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de empleado publico, nivel alto, cifrado	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
Certificado reconocido de empleado publico, nivel medio	critical, digitalSignature, nonRepudiation,	clientAuth, emailProtection	critical,CA:false

	keyEncipherment, dataEncipherment		
AC Camerfirma Express Corporate Server	critical, cRLSign, keyCertSign	-	critical,CA:true
Global Chambersign Root	critical, cRLSign, keyCertSign	-	critical,CA:true
AC Camerfirma	critical, cRLSign, keyCertSign	-	critical,CA:true
RACER	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado de Persona Física de Vinculación Pertenencia	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Representación	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física Ciudadano Emprendedor	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Factura Electrónica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Apoderado	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false

PERSONA FÍSICA al servei d'una ORGANITZACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en HSM	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Entidad de Certificación de la Administración Pública Andorrana	critical, cRLSign, keyCertSign	-	critical,CA:true
Certificado de Persona Física de Vinculación Pertenencia	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Representación	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de persona jurídica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física Ciudadano Emprendedor	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
Certificado de Persona Física de Vinculación Factura Electrónica	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false

Certificado de Persona Física de Vinculación Apoderado	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA PROFESSIONAL COL·LEGIAT en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei d'una ORGANITZACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – SIGNATURA	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l´ADMINISTRACIÓ en DSCF – XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical,CA:false
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
SEGELL D'EMPRESA (Persona Jurídica) en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM - Segell Electrònic	critical, nonRepudiation	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en HSM – IDENTITAT	critical, digitalSignature	clientAuth, emailProtection	critical,CA:false
REPRESENTANT PERSONA JURÍDICA en programari	critical, digitalSignature, keyEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en HSM	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false

Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic en programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical,CA:false

A pesar de que es posible técnicamente el cifrado de datos con los certificados, Camerfirma no se responsabiliza de los daños causados por la pérdida de control del titular de la clave privada necesaria para descifrar la información, excepto en el certificado emitido exclusivamente para este uso.

4.5.2 Uso de la clave pública y del certificado por la parte que confía

Las partes que confían deben acceder y usar la clave pública y el certificado según lo estipulado en esta DPC y según lo indicado en las "Condiciones de uso" bien en un documento físico o mediante su aceptación en el proceso de emisión.

4.6. Renovación del certificado

4.6.1 Circunstancia para la renovación del certificado

Un certificado debe renovarse antes de la fecha de caducidad del certificado a renovar. Una vez renovado Camerfirma emite el certificado renovado con fecha de inicio igual a la fecha de caducidad del certificado a renovar.

Los certificados de AC subordinada no se renuevan de forma automática, sino que deben emitirse en un procedimiento nuevo en base a una planificación previa, controlándose que el tiempo de vida del certificado siempre sea superior al máximo tiempo de validez de los certificados que se emiten bajo su rama jerárquica.

Los certificados de Operador de RA se renuevan cada dos años siempre y cuando no haya constancia de que ha dejado de ser Operador de RA.

Los certificados de ROOT, se emiten en un procedimiento nuevo mediante ceremonia elaborada al efecto.

Los certificados de OCSP se emiten periódicamente y no se establecen procesos de renovación.

4.6.2 Quién puede solicitar renovación

En aquellos certificados donde se permite la renovación, la autenticación del poseedor se realiza sobre la base de su certificado a renovar.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Antes de renovar un certificado, Camerfirma comprueba que la información utilizada para verificar la identidad y demás datos del Firmante y del poseedor de la clave sigue siendo válida.

En el caso de renovación de los certificados de entidad final de persona física, se permite la emisión de certificado sin presencia física hasta un periodo de 5 años desde el último registro presencial. Una vez superado el plazo marcado el Firmante deberá realizar un proceso de emisión presencial igual al realizado la primera emisión. Bajo estas prácticas, si en el momento de la renovación del certificado no han trascurrido más de 5 años, la presencia física del titular no será requerida.

Bajo estas prácticas, si cualquier información del Firmante o del poseedor de la clave ha cambiado, se debe realizar un nuevo registro y emisión, de acuerdo con lo establecido en las secciones correspondientes en este documento.

Camerfirma realiza las renovaciones de certificados emitiendo siempre nuevas claves, por lo tanto, el proceso técnico de emisión es igual al que se sigue cuando se realiza una nueva petición.

Camerfirma realiza cuatro avisos (30 días, 15 días, 7 días, 1 día) vía email al Firmante notificando que el certificado va a caducar.

El proceso de renovación se inicia a partir del correo de aviso de caducidad o directamente a través de la página Web de Camerfirma https://www.camerfirma.com/area-de-usuario/renovacion-de-certificados/. Este proceso requiere disponer del certificado válido a renovar.

- Una vez identificado con el certificado a renovar, el aplicativo presenta al Firmante los datos del certificado antiguo y le pide la confirmación de dichos datos. El aplicativo permite al Firmante modificar el email asignado al certificado. Si existen otros datos incorporados en el certificado que han cambiado, el certificado debe revocarse y proceder a realizar una emisión nueva.
- La petición se incorpora al aplicativo de RA donde el operador una vez revisados los datos, procede a pedir la emisión del certificado a la AC.
- Camerfirma como norma general emite un nuevo certificado tomando como inicio de validez la finalización del certificado a renovar. En algún caso se permite en los procesos de emisión a través de los servicios web, la renovación del certificado con fecha en el mismo momento de renovación, procediendo posteriormente a revocar el certificado a renovar.

4.6.4 Notificación de nueva emisión de certificado al suscriptor

La notificación de la emisión de un certificado renovado se producirá tal como se describe en la sección 4.3.2 de este documento.

4.6.5 Conducta que constituye la aceptación de un certificado de renovación

Según el apartado 4.4.1 de este documento.

4.6.6 Publicación del certificado de renovación por la CA

Según el apartado 4.4.2 de este documento.

4.6.7 Notificación de emisión de certificado por la CA a otras entidades

En algunos casos se envían certificados de entidad final a los supervisores nacionales que regulan las actividades de las autoridades de certificación.

Los certificados de OCSP se comunican a diferentes organismos gubernamentales que disponen de plataforma de validación de certificados.

Los certificados de ROOT y SubCA se notifican al supervisor nacional para su incorporación en la TSL. Adicionalmente a un repositorio de información gestionado por Mozilla, que incorpora información sobre autoridades de certificación – CCADB. Esta base de datos es utilizada por diversos programas comerciales para gestionar sus almacenes de confianza

4.7. Renovación de claves

Este es el procedimiento habitual de la renovación de los certificados de Camerfirma, por lo que todos los procesos descritos en la sección 4.6 se refieren a este método de renovación.

Camerfirma no permite la renovación de certificados sin renovación de claves.

4.7.1 Circunstancia para la renovación de claves (re-key) certificado

La renovación de certificados normalmente tendrá lugar como parte de la renovación de un Certificado.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

Según lo estipulado en 4.6.2

4.7.3 Procesamiento de solicitudes de cambio de claves del certificado

Según lo estipulado en 4.6.3

4.7.4 Notificación de nueva emisión de certificado al suscriptor

Según lo estipulado en 4.6.4

4.7.5 Conducta que constituye la aceptación de un certificado con nuevas claves (re-keyed)

Según lo estipulado en 4.6.5

4.7.6 Publicación del certificado con renovación de claves (re-keyed) por la AC

Según lo estipulado en 4.6.6

4.7.7 Notificación de emisión de certificado por la AC a otras entidades

Según lo estipulado en 4.6.7

4.8. Modificación de certificados

Cualquier necesidad de modificación de certificados implicará una nueva solicitud. Se realizará una revocación del certificado y una nueva emisión con los datos corregidos.

En el caso de tratarse de un proceso de sustitución de certificados, se considerará una renovación y así computa a la hora del cálculo de los años de renovación sin presencia física tal como marca la ley.

Se podrá proceder a la modificación de certificados como renovación cuando los atributos del suscriptor o del poseedor de claves que formen parte del control de unicidad previsto para esta política no hayan variado.

Si la solicitud de modificación se hace dentro del período ordinario previsto para la renovación del certificado, se procederá a realizar dicha renovación.

4.8.1 Circunstancia para la modificación del certificado

No aplicable.

4.8.2 Quién puede solicitar la modificación del certificado

No aplicable.

4.8.3 Procesamiento de solicitudes de modificación de certificados

No aplicable.

4.8.4 Notificación de la emisión de un nuevo certificado al suscriptor

No aplicable.

4.8.5 Conducta que constituye la aceptación del certificado modificado

No aplicable.

4.8.6 Publicación del certificado modificado por la CA

No aplicable.

4.8.7 Notificación de emisión de certificado por la CA a otras entidades

No aplicable.

4.9. Revocación y suspensión de certificados

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de este en función de alguna circunstancia distinta a la de su caducidad.

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

El periodo máximo de suspensión de un certificado es de 7 días naturales. En caso de llegar al periodo máximo de suspensión y el certificado no ha sido activado, el sistema automáticamente revoca definitivamente el certificado con causa "sin especificar".

La extinción de la vigencia de un certificado electrónico por causa de revocación o suspensión producirá efectos frente a terceros desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación (publicación de la lista de certificados revocados o consulta al servicio OCSP).

AC Camerfirma mantiene los certificados en la lista de revocación hasta el fin de su validez. Cuando esta situación se produce, se eliminan de la lista de certificados revocados. Camerfirma solo eliminará de la Lista de revocación un certificado cuando se produzca alguna de las dos siguientes situaciones.

- Caducidad del certificado
- Certificado revocado por causa de suspensión que una vez revisado se ha concluido que no se encuentran causas para su revocación definitiva.

No obstante, Camerfirma mantendrá la información sobre el estado de un certificado caducado en sus bases de datos y accesible a través del servicio de OCSP.

No está permitido en ningún caso bajo estas prácticas la utilización de un certificado revocado.

La respuesta de OCSP para un certificado revocado cuando caduca mantiene el estado de revocado y su causa.

Debido a las diferentes naturalezas de los servicios de OCSP y CRL, en caso de obtener respuestas distintas para un certificado caducado, se mantendrán como respuesta válida la ofrecida por el OCSP.

Para Camerfirma el servicio de consulta del estado de un certificado primario es el ofrecido por OCSP.

4.9.1 Causas de revocación

Como norma general se procederá a la revocación de un certificado por:

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto o incompleto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
- Falta de pago del certificado.

Por circunstancias que afectan la seguridad de la clave o del certificado

- Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
- Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta CPS.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del Firmante o del responsable de certificado.
- Acceso o utilización no autorizada, por un tercero, de la clave privada del Firmante o del responsable de certificado.
- El uso irregular del certificado por el Firmante o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.

Por circunstancias que afectan la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del Firmante o del responsable de certificado

Por circunstancias que afectan el Firmante o responsable del certificado.

- Finalización de la relación entre Entidad de Certificación y Firmante o responsable del certificado.
- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al Firmante o responsable del certificado.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
- Infracción por el Firmante o responsable del certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en esta Declaración de Prácticas de Certificación.
- La incapacidad sobrevenida o la muerte del Firmante o responsable del certificado.
- La extinción de la persona jurídica Firmante del certificado (sello electrónico), así como la finalidad de la autorización del Creador del Sello al responsable del certificado o la finalización de la relación entre el Creador del Sello y responsable del certificado.

- Solicitud del Firmante de revocación del certificado, de acuerdo con lo establecido en esta CPS.
- Resolución firme de la autoridad administrativa o judicial competente

Otras circunstancias

- La suspensión del certificado digital por un periodo superior al establecido en esta CPS.
- Por la emisión de un certificado que no cumpla los requisitos establecidos en esta declaración de prácticas de certificación
- La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección correspondiente en esta CPS.

Para justificar la necesidad de revocación que se alega se deberán presentar ante la RA o la AC los documentos correspondientes, en función de la causa que motiva la solicitud.

- Si solicita la revocación el titular del certificado o la persona física solicitante de un certificado de sello electrónico , deberá presentar una declaración firmada por él donde indique el certificado a revocar y la causa de esta solicitud e identificarse ante la RA

- Si la revocación la solicita un tercero deberá presentar una autorización bien del titular persona física bien del representante legal de la persona jurídica titular donde se indiquen además las causas por las que se solicita la revocación del certificado e identificarse ante la RA.

- Si solicita la revocación la Entidad vinculada al titular por causa de la terminación de la relación con éste, deberá acreditar dicha circunstancia (revocación de poderes, terminación contrato…) e identificarse ante la RA como facultado para representar a la Entidad.

Los Firmantes disponen de los códigos de revocación que pueden usar en los servicios de revocación vía Web o mediante llamada telefónica a los servicios de soporte.

4.9.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El Sujeto/Firmante

- El Solicitante responsable

- La Entidad (a través de un representante de la misma)

- La AR o la AC.

- También se contempla la posibilidad de que por parte de terceros o partes interesadas se pueda comunicar fraudes, malos usos, conductas inapropiadas, o datos erróneos, en cuyo caso, la AR o la AC podrá revocar el certificado tras comprobar la veracidad de dichas causas de revocación.

4.9.3 Procedimiento de solicitud de revocación.

Todas las solicitudes deberán realizarse:

- A través del Servicio de Revocación ONLINE, mediante el acceso al servicio de revocación localizado en la página de la Web de Camerfirma e introduciendo el PIN de Revocación.

  http://www.camerfirma.com/area-de-usuario/revocacion-de-certificados/

- A través de la personación física en la AR en horario de atención al público mostrando el **DNI** del Firmante/Suscriptor o Solicitante.

- Enviando a Camerfirma un documento firmado por un representante con capacidad de representación suficiente de la Entidad solicitando la revocación del certificado. Esta modalidad será la empleada para la revocación de los certificados de SubCA.

  Camerfirma mantiene en su página web toda la información relativa a los procesos de revocación de los certificados.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de Camerfirma. Estos servicios estarán disponibles las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de Camerfirma, Camerfirma realizará los mayores esfuerzos para asegurar que estos servicios no se encuentren inaccesibles durante un periodo máximo de 24 horas.

En caso de revocación por falta de pago, la RA o la AC requerirá previamente y en dos ocasiones sucesivas al Firmante a la dirección de correo electrónico de contacto, para que regularice esta situación en plazos de 8 días, a falta de lo cual, se procederá a la revocación con carácter inmediato.

4.9.4 Periodo de gracia de la solicitud de revocación

El periodo de revocación desde que Camerfirma o una AR tiene conocimiento autenticado de la revocación de un certificado esta se produce de manera inmediata, incorporándose en la próxima CRL a emitir y en la base de datos de la plataforma de gestión donde se alimenta el respondedor OCSP.

4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación

Camerfirma procesará una solicitud de revocación de forma inmediata a partir del procedimiento descrito en el punto 4.9.3

En las revocaciones producidas por una mala emisión del certificado se notificará previamente al titular para acordar los plazos de su sustitución.

Camerfirma en todo caso y bajo estas prácticas de certificación, puede realizar la revocación de un certificado de forma unilateral e inmediata por motivos de seguridad, sin que el titular pueda reclamar ningún tipo de indemnización por este hecho.

4.9.6 Requisitos de comprobación de la revocación por las partes que confían

Los Terceros que confían deben comprobar previamente a su uso, el estado de los certificados, debiendo comprobar en todo caso la última CRL emitida, que podrá descargarse en la URL que aparece en la extensión Punto de Distribución de CRL (*CRL Distribution Point*) de cada certificado.

Camerfirma emite siempre CRLs firmadas por la AC que ha emitido el certificado.

La CRL contiene un campo (*NextUpdate*) con la fecha de su próxima actualización.

4.9.7 Frecuencia de emisión de CRL's

CA	Frecuencia de emisión días	Duración días
Chambers of Commerce Root	**Máximo 365**	**365**
AC Camerfirma Certificados Camerales	Inmediato Máximo 1	2
AC CAMERFIRMA AAPP	Inmediato Máximo 1	2

Global Chambersign Root	**Máximo 365**	**365**
AC Camerfirma	**Máximo 365**	**365**
RACER	24 horas	48 horas
Entidad de Certificación de la Administración Pública Andorrana	24 horas	48 horas

4.9.8 Máxima latencia de CRL

Las CRL se publican cada 24 horas con una validez de 48 horas.

4.9.9 Disponibilidad de comprobación on-line de la revocación

AC proporciona un servicio on-line de comprobación de revocaciones vía HTTP en http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

También mediante consultas OCSP en:

https://www.camerfirma.com/servicios/respondedor-ocsp/.

Las direcciones de acceso a estos servicios vienen referenciadas en el certificado digital. Para las CRL y ARL en la extensión puntos de distribución de CRL "CRL Distribution Point" y la dirección de OCSP en la extensión Acceso a la Información de la Autoridad "Authority Information Access).

En los certificados puede aparecer más de una dirección de acceso a las CRL para garantizar su disponibilidad.

El servicio de OCSP se alimenta de las CRL emitidas por las diferentes autoridades de certificación (CA) o por accesos a la BBDD de la plataforma (EE). Los datos técnicos de acceso así como los certificados de validación de las respuestas OCSP se encuentran publicadas en la Web de Camerfirma https://www.camerfirma.com/servicios/respondedor-ocsp/

Estos servicios estarán disponibles las 24 horas del día los 7 días de la semana 365 días al año.

Camerfirma realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre inaccesible de forma continua más de 24 horas, siendo este un servicio crítico en las actividades de Camerfirma y por lo tanto tratado de forma adecuada en el Plan de contingencias y de continuidad de negocio.
La latencia de publicación en el servicio de OCSP de una revocación es de 1 hora

4.9.10 Requisitos de la comprobación on-line de la revocación

Para realizar la comprobación de una revocación el Tercero que confía deberá conocer el e-mail asociado al certificado que se desea consultar si se realiza mediante acceso Web o el número de serie si se comprueba mediante el servicio OCSP.

Las respuestas OCSP van firmadas por las AC que emite el certificado a consultar, por lo que es necesario dicho certificado para validar la respuesta. Los certificados actualizados se pueden encontrar en el link https://www.camerfirma.com/servicios/respondedor-ocsp/

4.9.11 Otras formas de divulgación de información de revocación disponibles

Los mecanismos que Camerfirma pone a disposición de los usuarios del sistema, estarán publicados en su página Web http://www.camerfirma.com/area-de-usuario/consulta-de-certificados

4.9.12 Requisitos especiales de revocación por compromiso de las claves

No estipulado

4.9.13 Circunstancias para la suspensión

Cuando se produce una suspensión, Camerfirma tendrá una semana para decidir el estado definitivo del certificado: (revocado o activo). En caso de no tener en este plazo toda la información necesaria para la verificación de su estado definitivo, Camerfirma revocará el certificado.

En el caso de producirse una suspensión del certificado, se envía un comunicado mediante email al Firmante/Suscriptor comunicando la hora de suspensión y la causa de la misma.

Si finalmente la suspensión no da lugar a la revocación definitiva y el certificado tiene que ser de nuevo activado, el Firmante/Suscriptor recibirá un correo indicando el nuevo estado del certificado.

El proceso de suspensión no se aplica a certificados

- De TSU
- De CA
- De Operador de AR.
- De OCSP

4.9.14 Quién puede solicitar la suspensión

Ver sección 4.9.2

4.9.15 Procedimiento de solicitud de suspensión

La solicitud de suspensión se realizará según mediante el acceso a la página correspondiente de la web de Camerfirma o mediante comunicación oral o escrita previamente autenticada. El suscriptor debe poseer el código de revocación para proceder a la suspensión del certificado.

4.9.16 Límites del periodo de suspensión

Un certificado no permanecerá suspendido más de 7 días.

Camerfirma supervisará mediante un sistema de alertas de la plataforma de gestión de certificados que el periodo de suspensión marcado por las Políticas correspondientes y esta CPS no se sobrepasa.

4.10. Servicios de comprobación del estado de los certificados

4.10.1 Características operacionales

Camerfirma dispone de un servicio de consulta de certificados emitidos y listas de revocación. Estos servicios están disponibles públicamente en su página Web: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

4.10.2 Disponibilidad del servicio

Los servicios de consulta están diseñados para garantizar una disponibilidad de 24 horas por día 7 días a la semana.

4.10.3 Características opcionales

No estipulado

4.11. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.
Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

4.12. Custodia y Recuperación de Claves

4.12.1 Política y prácticas de custodia y recuperación de claves

Para certificados en soporte hardware es el usuario quien genera y custodia la clave privada en la tarjeta criptográfica entregada por el prestador.

Para certificados emitidos en software Camerfirma almacena las claves de usuario en formato PKCS#12 con objeto de reenviarlas en caso de problemas en su descarga e instalación. Esta

información se almacena solo por 3 días naturales. Después de este periodo se eliminan dichas claves del sistema. Dichas claves no están incluidas en los servicios de copias de seguridad del sistema.

Para los certificados emitidos en dispositivo centralizado (CKC) Camerfirma almacena las claves generadas para el usuario en un dispositivo seguro HSM certificado al menos FIPS-140-2 nivel 3 o EAL 4+, proporcionando los mecanismos correspondientes para garantizar el control único de la clave.

Camerfirma almacena una copia de la clave privada del Firmante cuando esta se use "exclusivamente" para cifrado de datos.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

No estipulado.

5. CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES

5.1. Controles de seguridad física

Camerfirma está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001:2007 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

Camerfirma tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación certificados ofrece protección frente:

- Accesos físico no autorizados
- Desastres naturales
- Incendios
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura
- Inundaciones
- Robo
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso

Documento de referencia: IN-2005-01-01-Control de acceso físico

5.1.1 Ubicación y construcción

Las instalaciones de Camerfirma están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una caja de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas antihumedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

Documento de referencia: IN-2015-01-01-CPD

5.1.2 Acceso físico

El acceso físico a las dependencias de Camerfirma donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Cualquier persona externa debe estar acompañada por un responsable de la organización cuando esta se encuentre por cualquier motivo dentro de áreas restringidas.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un registro de auditoría de entradas y salidas automático.

El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

El acceso a los sistemas de certificación está protegido con 4 niveles de acceso. Edificio, Oficinas, CPD y Sala criptográfica.

5.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones de Camerfirma disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 Exposición al agua

Las instalaciones de Camerfirma están ubicadas en una zona de bajo riesgo de inundación y en una primera planta. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

Los dispositivos criptográficos, y soportes que almacenen claves de las Entidades de Certificación, cuentan con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

5.1.6 Sistema de almacenamiento.

Cada Medio de Almacenamiento desmontable (cintas, cartuchos, CD, discos, etc.) permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento se guarda en armarios ignífugos o bajo llave permanentemente en requiriéndose autorización expresa para su retirada.

5.1.7 Eliminación de residuos

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga.

Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

Documento de referencia: IN-2005-01-03-Seguridad medioambiental

5.1.8 Backup externo

Camerfirma utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro operacional.

Se requiere al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

Documento relacionado: IN-2005-04-06-Procedimiento de Backups de ficheros críticos

5.2. Controles procedimentales

5.2.1 Roles de confianza

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación, y con una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tienen en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

Auditor Interno:
Responsable del cumplimiento de los procedimientos operativos. Es una persona externa al departamento de Sistemas de Información.

Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

Administrador de Sistemas:
Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación.

Las tareas de administrador de sistemas son incompatibles con las tareas de certificación y no pueden llevar a cabo tareas de auditores de operaciones.

Administrador de AC.
Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.

Las tareas del administrador de AC son incompatibles con las tareas de certificación y sistemas.

Operador de AC.
Responsable necesario conjuntamente con el Administrador de AC de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.

Las tareas de operador de AC son incompatibles con las de administrador de AC y no puede realizar tareas de auditor ni auditor interno.

Operador de RA:

Persona responsable de aprobar las peticiones de certificación realizadas por el Firmante.

Las operaciones de operador de RA son incompatibles con las de administrador de RA ni puede realizar tareas de auditoria interna ni externa.
Operador de revocación:
Las tareas del operador de revocación son incompatibles con las tareas de Auditoria

Responsable de Seguridad:
Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de Camerfirma. Debe encargarse aspecto relacionado con la seguridad de la información: lógica, física, redes, organizativa, etc.

Documento de referencia: IN-2005-02-07 Funciones y responsabilidad del personal

5.2.2 Número de personas requeridas por tarea

Camerfirma garantiza al menos **dos personas para realizar las tareas clasificadas como sensibles**. Principalmente en la manipulación del dispositivo de custodia de las claves de AC Root y AC intermedias.

5.2.3 Identificación y autentificación para cada rol

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación

5.2.4 Roles que requieren separación de tareas

El documento interno IN-2016-03-01 ficha de perfil de puesto refleja las tareas asignadas a los diferentes perfiles con una tabla de segregación de roles.

	Responsable de Seguridad	Administracion de Sistemas	Oeración de sistemas	Auditor Plataforma CA	Especialidsta Validacion SSL	Operador RA
Responsable de Seguridad		SI	NO	SI	SI	SI
Administracion de Sistemas	NO		NO	NO	NO	NO
Operación de Sistemas	NO	NO		NO	NO	NO
Auditor Plataformas CA	NO	NO	NO		SI	SI
Especialidsta Validacion SSL	NO	NO	NO	SI		SI
Operador RA	NO	NO	NO	NO	SI	

5.2.5 Arranque y parada del sistema de gestión PKI.

El sistema de PKI se compone de los siguientes módulos:

Módulo de Gestión de AR, para lo cual se activarán o desactivarán los servicios del gestor de páginas especifico.
Actualmente AC Camerfirma gestiona dos plataformas técnicas dietitas para cada una de las jerarquías, aunque el apagado se realiza de la misma forma desactivando los servicios del gestor de páginas.

Módulo de gestión de solicitudes, para lo cual se activará o desactivará los servicios del gestor de páginas específico.

Módulo de gestión de claves, ubicado en el equipo HSM. Se activa o desactiva mediante encendido físico.

Módulo de BBDD, Gestión centralizada de los certificados y CRL gestionados, OCSP y TSA. Arranque y parada del servicio específico del Gestor de BBDD.

Módulo OCSP. Servidor de respuestas de estado de los certificados en línea. Arranque y parada del servicio de sistema encargado de esta tarea.

Módulo TSA. Servidor de sellos de tiempos. Arranque y parada del servicio

El proceso de apagado de módulos seguiría la secuencia:

- Módulo de solicitud
- Módulo de AR
- Módulo OCSP
- Módulo TSA
- Módulo BBDD
- Módulo gestión de claves.

Se realizará el encendido en proceso inverso.
Documento interno de referencia: IN-2005-05-01-Procedimiento para el apagado manual de equipos.

5.3. Controles del personal

5.3.1 Calificaciones, experiencia y requisitos de autorización

Todo el personal que realiza tareas calificadas como confiables lleva al menos **un año** trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza se encuentra libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

Camerfirma se asegura de que el personal de registro o Administradores de AR es confiable y pertenece a una Cámara de Comercio o del organismo delegado para realizar las tareas de registro.

El Administrador de AR habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, Camerfirma retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

Camerfirma no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación, hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad

Documentación de referencia:

- IN-2005-02-07 Funciones y responsabilidad del personal.
- IN-2005-02-17-Gestión Recursos humanos
- IN-2008-00-09-Registros de Formación
- IN-2006-02-03-Organizacion para la Seguridad

5.3.2 Procedimientos de comprobación de antecedentes

Camerfirma dentro de sus procedimientos de RRHH realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

Camerfirma nunca asigna tareas confiables a personal con menos de una antigüedad de un año.

En la solicitud para el puesto de trabajo se informa sobre la necesidad de someterse a una investigación previa y se advierte que la negativa a someterse a la investigación implicará el rechazo de la solicitud. Asimismo consentimiento inequívoco del afectado para la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la legislación de protección de datos de carácter personal.

5.3.3 Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado en los términos que establecen las Políticas de Certificación. Existe un plan de formación que forma parte de los controles UNE-ISO/IEC 27001:2007.

Se realizará una formación específica a los operadores de registro que validen certificados de servidor seguro EV respecto a la norma específica que regulan la emisión de estos certificados.

La formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía pública de certificación.
- Versiones de hardware y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter persona

5.3.4 Requerimientos y frecuencia de la actualización de la formación

Camerfirma realiza los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas.

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado

5.3.6 Sanciones por acciones no autorizadas

Camerfirma dispone de un régimen sancionador interno, descrito en su política de RRHH, para su aplicación cuando un empleado realice acciones no autorizadas pudiéndose llegar a su cese.

5.3.7 Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de confidencialidad y los requerimientos operacionales empleados por Camerfirma. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la CPS, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, la entidad de certificación será responsable en todo caso de la efectiva ejecución.

Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto de Camerfirma debiendo obligarse los terceros a cumplir con los requerimientos exigidos por Camerfirma.

Documentación de referencia:
- IN-2006-05-02-Clausulas exigible a desarrolladores externos,
- IN-2005-02-17-Gestión Recursos humanos

5.3.8 Documentación proporcionada al personal

Camerfirma pone a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, en particular la normativa de seguridad y la CPS.

Esta documentación se encuentra en un repositorio interno accesible por cualquier empleado de Camerfirma, en el repositorio existe una lista de documentos de obligado conocimiento y cumplimiento.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

Documentación de referencia IN-2005-02-17-Gestión Recursos humanos

5.4. Procedimientos de registro de eventos

Camerfirma está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001:2007que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

5.4.1 Tipos de eventos registrados

Camerfirma registra y guarda los registros de auditoría de todos los eventos relativos al sistema de seguridad de la AC.

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- 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.
- Acceso físico a los registros de auditoría.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.

Camerfirma también conserva, ya sea manualmente o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física y vulnerabilidades en las infraestructuras que dan soporte a la emisión y gestión de certificados

Camerfirma mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de registros de auditoría.
- Que los ficheros de registros de auditoría no se reescriben.

- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de registros de auditoría se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.2 Frecuencia de tratamiento de registros de auditoria

Camerfirma revisa sus registros de auditoría cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

5.4.3 Periodos de retención para los LOGs de auditoria

Camerfirma almacena la información de los registros de auditoría al menos durante cinco años.

5.4.4 Protección de los registros de auditoría

Los registros de auditoría de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de registros de auditoría está reservado solo a las personas autorizadas.

Los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de registros de auditoría.

5.4.5 Procedimientos de copia de respaldo de los registros de auditoría

Camerfirma dispone de un procedimiento adecuado de copia de respaldo de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de copia de respaldo de los registros de auditoría.

Camerfirma tiene implementado un procedimiento de back up seguro de los logs de auditoría, realizando semanalmente una copia de todos los registros de auditoría en un medio externo.

Adicionalmente se mantiene copia en centro de custodia externo.

Documentación de referencia: IN-2005-04-10-procedimiento de gestión de registros de auditoría.

5.4.6 Sistema de recogida de información de auditoria

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, la red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado, todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación al sujeto causa del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será necesario enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de Camerfirma. Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación UNE-ISO/IEC 27001 que está reflejados en el documento CONF-2005-05-01 – Análisis de riesgos. En este documento se especifican los controles implantados para garantizar los objetivos de seguridad requeridos.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

Mensualmente Camerfirma ejecuta un análisis de los sistemas con objetivo de detectar actividades sospechosas. Este informe es ejecutado por una empresa externa incorpora:

- Detección de intrusión - IDS (HIDS)
- Sistema de control de integridad OSSEC
- SPLUNK. Inteligencia operacional.
- Informe correlación de eventos.

Camerfirma corrige cualquier problema reportado y es registrado por el departamento de sistemas.

5.5. Archivo de registros

5.5.1 Tipo de archivos registrados.

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por la AC o por las RAs:

- Todos los datos de auditoría de sistema. PKI, TSA, OCSP y plataforma centralizada de claves (CKC) incorporando los eventos de firma realizados.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y RA. Los datos relativos a su identificación y su ubicación.
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación

Camerfirma responsable del correcto archivo de todo este material.

5.5.2 Periodo de retención para el archivo

Los certificados, los contratos con los Sujetos/Firmantes y cualquier información relativa a la identificación y autenticación del Sujeto/Firmante serán conservados durante al menos quince años.

Las versiones antiguas de la documentación también son conservadas, por un periodo de quince años por AC Camerfirma, pudiendo ser consultadas, por causa razonada por los interesados.

5.5.3 Protección del archivo

Camerfirma asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

Documento relacionado: IN-2005-04-01- Procedimiento de gestión de logs

5.5.4 Procedimientos de copia de respaldo del archivo

Camerfirma dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

Documento relacionado: IN-2005-04-01- Procedimiento de gestión de logs

Camerfirma como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realiza copias de respaldo completas semanalmente para casos de recuperación de datos.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable vía NTP desde el ROA, GPS y sistemas de sincronización vía Radio.

Camerfirma dispone de un documento de seguridad informática donde describe la configuración de los parámetros de fecha y hora de los equipos utilizados en la emisión de certificados.

Documento relacionado: IN-2006-04-01-Sincronizacion de tiempos

5.5.6 Sistema de recogida de información de auditoria

Camerfirma dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

Documentación de referencia: IN-2005-04-10-procedimiento de gestión de logs

5.5.7 Procedimientos para obtener y verificar información archivada

Camerfirma dispone de un documento de seguridad informática donde se describe el proceso para verificar que la información archivada es correcta y accesible.

Documento relacionado: IN-2005-04-06-Procedimiento de Backups de ficheros críticos

5.6. Cambio de clave

El cambio de claves de entidad final es realizado mediante la realización de un nuevo proceso de emisión (ver apartado correspondiente de esta CPS).

En CA (Root CA, SubCA). Antes de que el certificado de la AC caduque se realizará un cambio de claves. El certificado a actualizar de la AC y su clave privada solo se usará para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará un nuevo certificado de AC con una clave privada nueva y un CN (*common name*) distinto al del certificado de la AC a sustituir.

También se realizará cambio de certificado de una AC cuando el estado del arte criptográfico (algoritmos, tamaño de claves, etc.) lo requiera.

Documento de referencia: IN-2005-04-04-Procedimiento de cambio de claves.

5.7. Recuperación en caso de compromiso de la clave o desastre

El caso de compromiso de la clave raíz se toma como un caso particular en el documento de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos del sector privado y público. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos de reconocimiento. El documento de contingencia y continuidad de negocio incorpora estos términos puramente técnicos y operativos para que las nuevas claves estén disponibles, pero no así su reconocimiento por terceros.

El compromiso de los algoritmos o los parámetros asociados utilizados en la generación de certificados digitales o servicios asociados se incorporan también en el plan de contingencias y continuidad de negocio.

5.7.1 Procedimientos de gestión de incidencias y compromisos

Camerfirma ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario un centro de datos alternativo como parte de la certificación UNE-ISO/IEC 27001:2007

El plan de continuidad y contingencias está redactado en el documento CONF-2003-00-01 Continuidad y Disponibilidad.

5.7.2 Corrupción de recursos, aplicaciones o datos

Si algún equipo se daña o deja de funcionar pero las claves privadas no se destruyen, la operación debe restablecerse lo más rápido posible, dando prioridad a la capacidad de generar información del estado del certificado según el plan de recuperación de desastres de Camerfirma.

5.7.3 Compromiso de clave privada de la entidad

El Plan de contingencias enmarcado en la certificación UNE-ISO/IEC 27001:2007 de Camerfirma trata el compromiso de la clave privada de la AC como una situación de desastre

En caso de compromiso de una clave raíz:

- Informará a todos los Firmantes/Suscriptores, Tercero que confía y otras ACs con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

5.7.4 Continuidad del negocio después de un desastre

Camerfirma restablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con el plan de contingencias y continuidad de negocio enmarcado en la certificación UNE-ISO/IEC 27001:2007 indicando un restablecimiento en las 24 horas siguientes.

Camerfirma dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descrito en el plan de continuidad de negocio.

5.8. Cese de la AC o AR

Antes del cese de su actividad Camerfirma realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras ACs con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de seis meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá 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 AC serán destruidas o deshabilitadas para su uso.
- Camerfirma mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.

Todas estas actividades estarán recogidas en detalle en el documento interno CONF-2003-00-01 Plan de Continuidad y disponibilidad y Cese de Actividad de AC Camerfirma SA.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación del par de claves

6.1.1 Generación del par de claves

Los equipos usados por Camerfirma son nCipher. Estos dispositivos albergaran claves raíces y están certificados FIPS 140-2, en su nivel 3.

Las claves raíz se generan y gestionan en un equipo fuera de línea en una sala criptográfica.

Documento de referencia CONF-00-2012-02-Script de generación de CA ROOT xxxx siendo "xxxx" el año correspondiente a la creación de las claves.

La creación de claves de SubCAs se genera en equipos HSM donde se albergarán para su correspondiente uso. El certificado emitido por la calve raíz se realiza en una sala criptográfica segura.

CA	Longitud de claves	Algoritmo de firma	Año creación	Caducidad
Chambers of Commerce Root	2.048 bits	Sha1WithRSAEncryption	2.003	30/09/2037
AC Camerfirma Express Corporate Server	2.048 bits	Sha1WithRSAEncryption	2.007	09/02/2034
AC Camerfirma Certificados Camerales	2.049 bits	Sha1WithRSAEncryption	2.004	09/02/2034
AC CAMERFIRMA AAPP	2.048 bits	Sha1WithRSAEncryption	2.010	20/02/2022
Global Chambersign Root	2.048 bits	Sha1WithRSAEncryption	2.003	30/09/2037
AC Camerfirma	2.048 bits	Sha1WithRSAEncryption	2.003	14/11/2033
RACER	2.048 bits	Sha1WithRSAEncryption	2.003	04/12/2023

Más información en http://www.camerfirma.com/area-de-usuario/politicas-y-practicas-de-certificacion/

Documentación de referencia:
- CONF-00-2012-01 ACTAS de ceremonias de creación de claves.
- CONF-00-2012-02/04 SCRIPTS de Generación de claves.
- CONF-00-2012-05 Informe Auditores.
- CONF-00-2012-03 Reparto de claves entre operadores.

6.1.1.1 Generación del par de claves del suscriptor

Las claves del Sujeto/Firmante pueden ser creadas en por el mismo mediante dispositivos hardware (QSCD) o software autorizados por Camerfirma o pueden ser creadas por Camerfirma en formato software PKCS#12.

En certificados SSL/TLS el cliente genera el par de claves bajo el control del sistema gestor de páginas correspondiente.

Si el certificado requiere un dispositivo de creación de firma este certificado solo se utilizará únicamente con dichos dispositivos para realizar firmas electrónicas.

La plataforma de gestión STATUS genera con sus propios recursos una contraseña aleatoria robusta y una clave privada protegida con dicha contraseña usando el algoritmo 3DES. A partir de esa clave privada genera una petición de firma de certificado en formato PKCS#10. Con esa petición la AC realiza la firma del certificado del Firmante. El certificado es entregado al usuario en un fichero PKCS#12 en el que se incluye el propio certificado y la clave privada asociada a él. La contraseña de la clave privada y del fichero PKCS#12 nunca está en claro en el sistema.

Las claves son generadas usando el algoritmo de clave pública RSA.

Las claves también pueden ser creadas en un sistema remoto usando la capa de servicios WEB para generar una solicitud PKCS#10 y la recogida del PKCS#7 correspondiente.

En un sistema de gestión centralizada de claves CKC, las claves son generadas en un HSM que cumple la normativa FIPS-140-2 L3 Las claves tienen una longitud mínima de 2048 bits.

6.1.1.2 Hardware/software de generación de claves

Las claves de los Firmantes/Suscriptores pueden ser generadas por ellos mismos en un dispositivo autorizado por Camerfirma. Ver 6.1.1.1

Las claves de ROOT se ha utilizan un dispositivo criptográfico que cumple las especificaciones FIPS 140-2 level 2 y level 3.

6.1.2 Entrega de la clave privada al firmante

Ver 3.2.1

6.1.3 Entrega de la clave pública al emisor del certificado

El envío de la clave pública a Camerfirma para la generación del certificado cuando el circuito así lo requiera, se realiza mediante un formato estándar preferiblemente en formato PKCS#10.

6.1.4 Entrega de la clave pública de la AC a los usuarios

El certificado de la AC y su *fingerprint* (huella digital) estarán a disposición de los usuarios en la página Web de Camerfirma https://www.camerfirma.com/area-de-usuario/descarga-de-claves-publicas/

6.1.5 Tamaño de las claves

Las claves privadas del Firmante/Suscriptor están basadas en el algoritmo RSA con una longitud mínima de 2048 bits.

El periodo de uso de la clave pública y privada varía en función del tipo de certificado. Ver apartado 6.1.1.

6.1.6 Parámetros de generación de la clave pública y control de calidad.

La clave pública de la AC Raíz y de la AC Subordinada y de los certificados de los suscriptores está codificada de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA

- Tamaño de claves = mínimo 2048 bits
- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-256

6.1.7 Propósitos de uso de claves

Todos los certificados emitidos contienen los atributos "KEY USAGE" y "EXTENDED KEY USAGE", tal como se define en el estándar X.509v3. Más información disponible en la sección 7.1.2.

6.2. Protección de la clave privada y estándares para los módulos criptográficos

6.2.1 Controles y estándares de módulos criptográficos

6.2.1.1 Clave privada de la AC

La clave privada de firma de las AC raíz y las AC subordinadas son mantenidas en un dispositivo criptográfico que cumple las especificaciones FIPS 140-2 nivel 3.

Cuando la clave privada de la AC está fuera del dispositivo esta se mantiene cifrada.

Existe un back up de la clave privada de firma de la AC, que es almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro.

Las copias de back up de la clave privada de firma de la AC están almacenadas de forma segura. Este procedimiento se describe en detalle en las políticas de seguridad de Camerfirma.

Las claves de AC subordinadas externas se mantienen en dispositivos que cumplen al menos FIPS 140-2 nivel 3.

- CONF-2016-04-02-Proteccion y activación de claves de CA Online

- CONF-2012-04-10 - Script Ceremonia de emisión de certificados.

6.2.1.2 **Clave privada del suscriptor**

La clave privada del suscriptor se puede almacenar en un dispositivo software o hardware.

Cuando se almacene en formato software Camerfirma ofrecerá las instrucciones de configuración adecuada para un uso seguro.

En un sistema de gestión centralizada de claves CKC, las claves son generadas en un HSM certificado FIPS-140-2 L3

Respecto a los dispositivos criptográficos distribuidos por Camerfirma para albergar certificados electrónicos (no cualificados), cumplen todos con los requisitos de dispositivos cualificados de creación de firma cualificados y por lo tanto serían aptos para la generación de firma cualificada siempre y cuando fueran objeto de una Evaluación de conformidad al Reglamento eIDAS (cabe precisar que dicha CPS no incluye Autoridades de certificación que hayan sido objeto de una Evaluación de Conformidad).

La información respecto al proceso de creación y custodia de claves que utiliza Camerfirma se incorpora en el propio certificado digital, mediante el OID correspondiente permitiendo a la Parte Usuaria actuar en consecuencia.

6.2.2 Control multipersonal (n de entre m) de la clave privada

Se requiere un control multipersonal para la activación de la clave privada de la AC. En el caso de esta CPS, en concreto existe una política de 2 de 4 personas para la activación de las claves.

Documentación de referencia: CONF-00-2012-03-Reparto de claves entre operadores

6.2.3 Depósito de clave privada

Camerfirma no almacena ni copia las claves privadas de los titulares.

Excepciones:

- En caso de certificados para cifrado de información Camerfirma guarda una copia de dicha clave.

6.2.4 En un sistema de gestión centralizada de claves CKC, las claves son generadas en un HSM certificado FIPS-140-2 L3Copia de seguridad de la clave privada

Camerfirma realiza una copia de back up de las claves privadas de la ACs que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de esta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del Firmante en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación tal como se indica en el manual de instalación de claves en software.

Las claves del Firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

En un sistema de gestión centralizada de claves CKC, se pueden realizar copias de seguridad de las claves del firmante en los términos marcados por la reglamentación correspondiente.

Camerfirma guarda actas de los procesos de gestión de las claves privadas de AC.

Documentación de referencia: CONF-00-2012-01-Acta de backup de las claves de las CA root.

6.2.5 Archivo de la clave privada

Las claves privadas de las ACS son archivadas por un periodo de 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

El Firmante podrá almacenar las claves entregadas en software durante el periodo de duración del certificado, posteriormente deberá destruirlas asegurándose antes de que no tiene ninguna información cifrada con la clave pública.

Solo en caso de certificados de cifrado el Firmante podrá almacenar la clave privada el tiempo que crea oportuno. En este caso Camerfirma también guardará copia de la clave privada asociada al certificado de cifrado.

AC Camerfirma pone a disposición de los titulares de certificados cuya clave privada sea generada por el prestador desde el momento de la entrega de dicho certificado la descarga del fichero PKCS#12, que contiene dicha clave privada y su certificado asociado, durante tres días hábiles.

Camerfirma guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.6 Introducción de la clave privada en el módulo criptográfico.

Las claves de CA ROOT se mantienen almacenadas en el módulo criptográfico PCI con el equipo asociado desconectado cuando no se esté realizando ninguna operación.

Las claves de las CAs intermedias se almacenan en equipos HSM de red en línea, de forma que se puedan acceder desde los aplicativos de PKI para la generación de certificados.

En un sistema de gestión centralizada de claves del firmante CKC según consta en la descripción en el manual del fabricante del dispositivo.

6.2.7 Almacenamiento de clave privada en el módulo criptográfico

Las claves de CA ROOT se mantienen almacenadas en el módulo criptográfico PCI con el equipo asociado desconectado cuando no se esté realizando ninguna operación.

Las claves de las CAs intermedias se almacenan en equipos HSM de red en línea, de forma que se puedan acceder desde los aplicativos de PKI para la generación de certificados.

En un sistema de gestión centralizada de claves del firmante CKC según consta en la descripción en el manual del fabricante del dispositivo.

6.2.8 Método de activación de la clave privada.

El acceso a la clave privada del suscriptor se realiza por medio de una clave de activación que conocerá solamente el suscriptor y que evitará tenerlo por escrito.

La clave de la AC Root se activa por un proceso de m de n. Ver 6.3.1 **¡Error! No se encuentra el origen de la referencia.**

La activación de las claves privadas de la ACs Intermedias son gestionadas por el aplicativo de gestión.

En un sistema de gestión centralizada de claves del firmante CKC según consta en la descripción en el manual del fabricante del dispositivo.

Documentación de referencia: CONF-2008-04-09-Acceso_PKCS#11_CAS_online

Camerfirma guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.9 Método de desactivación de la clave privada

Para los certificados en tarjeta, la clave privada del suscriptor quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

Cuando la clave esté en soporte software, podrá ser desactivada mediante el borrado de dichas claves de la aplicación correspondiente en la que estén instaladas.

Para la desactivación de la clave privada de la AC se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Para claves de entidad Root, AC, subCA, TSU, se realizará una ceremonia criptográfica de la que se elaborará el acta correspondiente.

En un sistema de gestión centralizada de claves del firmante CKC según consta en la descripción en el manual del fabricante del dispositivo.

6.2.10 Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves se emitirá una revocación del certificado de la clave pública asociada a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de las ACs de las Jerarquías. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del Firmante en software se podrán destruir mediante el borrado de estas siguiendo las instrucciones de la aplicación que las alberga.

Las claves del Firmante en hardware podrán ser destruidas mediante un software especial en los puntos de Registro o en la AC.

En un sistema de gestión centralizada de claves del firmante CKC según consta en la descripción en el manual del fabricante del dispositivo.

Camerfirma guarda actas de los procesos de gestión de las claves privadas de AC.

6.2.11Calificación del módulo criptográfico

Los módulos criptográficos están certificados FIPS-140-2 nivel 3 son manejados por al menos dos operadores en un modelo n de m. Los equipos están albergados en entornos seguros. El módulo criptográfico que almacenas las claves de Root se gestiona dentro de una sala criptográfica aislada y desconectada. Los módulos criptográficos que almacenan las claves de SubCA se almacenan en entornos seguros dentro de un CPD siguiendo normativa ISO27001.

En un sistema de gestión centralizada de claves CKC, las claves son generadas en un HSM certificado FIPS-140-2 L3

6.3. Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

La AC, en cumplimiento de lo establecido por el artículo 20 f) de la LFE 59/2003 mantendrá sus archivos por un periodo mínimo de quince (15) años siempre y cuando la tecnología de cada momento lo permita. Dentro de la documentación a custodiar se encuentran los certificados de clave pública emitidos a sus suscriptores y los certificados de clave pública propios.

6.3.2 Periodo de uso para las claves públicas y privadas

La clave privada no debería ser usada después del periodo de validez del certificado de clave pública asociada.

La clave pública o su certificado de cave publica puede ser usada como mecanismo de verificación de datos cifrados con la clave pública fuera del ámbito temporal para labores de validación.

Una clave privada podrá usarse fuera del periodo marcado por el certificado digital correspondiente, únicamente para la recuperación de datos cifrados.

6.4. Datos de activación

6.4.1 Generación y activación de los datos de activación

Los datos de activación de la clave privada de usuario se generan de diferente forma según el tipo de certificado

En software. El certificado se genera por el prestador y se entrega en un fichero estandarizado PKCS#12 protegido por una contraseña generada por el aplicativo de gestión y entregada al sujeto mediante el correo asociado al certificado digital.

En Dispositivo hardware. Las tarjetas utilizadas por Camerfirma se generan en el puesto de registro protegidas con un PIN y PUK calculado de fábrica. Esta información es enviada por la plataforma de gestión al sujeto mediante el correo asociado al certificado digital. El sujeto dispone de un software para cambiar el PIN y PUK de su tarjeta.

En Dispositivo hardware (HSM) de tercero. AC Camerfirma homologa dispositivos de terceros, aunque estas disponen de una gestión independiente. Las claves se generan en una ceremonia independiente y se entrega a Camerfirma una solicitud de emisión de certificado conjuntamente con el acta de la ceremonia.

En la plataforma de gestión centralizada, las claves se generan en un dispositivo criptográfico HSM protegido por una clave maestra del dispositivo y por los datos de activación de la clave generada y conocida solo por el propio titular del certificado asociado. La plataforma permite activar un doble control de activación vía OTP.

6.4.2 Protección de los datos de activación

Los datos de activación son comunicados al sujeto por un canal independiente a la plataforma de gestión PKI. AC Camerfirma no almacena dicha información custodiada en su base de datos cuando hablamos de certificados en formato software o hardware. En la plataforma centralizada no los almacenamos siendo conocidos y custodiados por el titular. Los datos pueden ser enviados de nuevo al sujeto bajo solicitud previa al correo asociado al certificado, y serán eficaces siempre que el usuario no haya realizado un cambio en ellos previamente.

En un sistema de gestión centralizada de claves del firmante CKC según consta en la descripción en el manual del fabricante del dispositivo.

6.4.3 Otros aspectos de los datos de activación

No estipulados.

6.5. Controles de seguridad informática

Camerfirma emplea sistemas fiables para ofrecer sus servicios de certificación. Camerfirma ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos

informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se sigue el esquema de certificación sobre sistemas de gestión de la información ISO 270001

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Camerfirma, en los siguientes aspectos:

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento correcto del sistema.
4. Configuración de Usuarios y permisos.
5. Configuración de eventos de Log.
6. Plan de backup y recuperación.
7. Configuración antivirus
8. Requerimientos de trafico de red

6.5.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de Camerfirma incluye 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 expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2 Valoración de la seguridad informática

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

6.6. Controles de seguridad del ciclo de vida

Cuando las claves criptográficas asociadas a un certificado se almacenan en un dispositivo hardware, este es siempre un dispositivo cualificado de creación de firma cumpliendo el anexo II de eIDAS. El dispositivo hardware puede ser una tarjeta criptográfica, token USB o HSM.

Respecto a los dispositivos hardware

a) Los dispositivos hardware son preparados y estampadas por un proveedor externo.
b) La gestión de distribución del soporte la realiza el proveedor externo que lo distribuye a las autoridades de registro para su entrega al Firmante.
c) El Firmante o la RA utiliza el dispositivo para generar el par de claves y enviar la clave pública a la AC.
d) La AC envía un certificado de clave pública al Firmante o la RA que es introducido en el dispositivo.
e) El dispositivo es reutilizable y puede mantener de forma segura varios pares de claves.
f) El dispositivo queda en propiedad del sujeto/Firmante.

6.6.1 Respecto a los dispositivos utilizados en la plataforma de gestión centralizada de claves: El dispositivo que almacena dichas claves está certificado FIPS-104-2 nivel 3 o EAL4+ Controles de desarrollo del sistema

Camerfirma posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

Como respuesta a los análisis de intrusión y vulnerabilidades se realizan las adaptaciones de los sistemas y aplicaciones que pueden tener problemas de seguridad y a las alertas de seguridad recibidas desde los servicios de seguridad gestionadas contratados con terceros, se ejecutan los RFC (*Request for Changes*) correspondientes para la incorporación de los parches de seguridad o la actualización de las versiones con problemas.

En el RFC se incorporan y se documentan las medidas tomadas para la aceptación, ejecución o la denegación de dicho cambio.

En los casos que la ejecución de la actualización o corrección de un problema incorpore una situación de vulnerabilidad o un riesgo importante se incorpora en el análisis de riesgos y se ejecutan controles alternativos hasta que el nivel de riesgo sea asumible.

Documentación de referencia:

- IN-2006-05-02-Clausulas exigible a desarrolladores externos
- IN-2006-03-04-Control de cambios a Sistemas y Software

6.6.2 Controles de gestión de la seguridad

6.6.2.1 Gestión de seguridad

Camerfirma desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad.

Para realizar esta función dispone de un plan de formación anual.

Camerfirma exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.2 Clasificación y gestión de información y bienes

Camerfirma mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

Documentación de referencia: IN-2005-02-15-Clasificación e Inventario de Activos

La política de seguridad de Camerfirma detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

Documentación de referencia: IN-2005-02-04-Política de Seguridad

6.6.2.3 Operaciones de gestión

Camerfirma dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En el documento de seguridad de Camerfirma se desarrolla en detalle el proceso de gestión de incidencias.

Documentación de referencia: IN-2010-10-08 Gestión de incidencias

Camerfirma tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Documentación de referencia: IN-2005-02-07 Funciones y responsabilidad del personal

Tratamiento de los soportes y seguridad
Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Documentación de referencia:
- CONF-2006-01-04-Procedimiento de Registro de Entradas y Salidas de Soportes
- IN-2005-02-15-Clasificación e Inventario de Activos

Planificación del sistema
El departamento de Sistemas de la Camerfirma mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Documentación relacionada:

- IN-2010-10-10 Gestión de Configuración

- IN-2010-10-05 Gestión de la capacidad
- IN-2010-10-03 Gestión de la Disponibilidad
- IN-2010-10-01 Gestión del Nivel de Servicio
- IN-2010-10-00 Manual de Gestión de Servicios de TI
- IN-2010-10-13 Planificación de Nuevos Servicios

Reportes de incidencias y respuesta
Camerfirma dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Documentación de referencia: IN-2010-10-08 Gestión de incidencias

Procedimientos operacionales y responsabilidades
Camerfirma define actividades, asignadas a personas con un rol de confianza, distintas a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

Documentación de referencia: IN-2005-02-07 Funciones y responsabilidad del personal

6.6.2.4 Gestión del sistema de acceso

Camerfirma realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

Documentación de referencia: IN-2011-04-10 Control de accesos a red.

En particular:

AC General

a) Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
b) Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
c) Camerfirma dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
d) Camerfirma dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
e) Cada persona tiene asociado un rol para realizar las operaciones de certificación.
f) El personal de Camerfirma es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la AC.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de AC.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5 Gestión del ciclo de vida del hardware criptográfico

Camerfirma se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

Camerfirma registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Camerfirma realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de la AC así como sus modificaciones y actualizaciones son documentadas y controladas.

Camerfirma posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.6.3 Evaluación de la seguridad del ciclo de vida

No estipulado

6.7. Controles de seguridad de la red

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

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

La política empleada para la configuración de los sistemas y elementos de seguridad es partir de un estado inicial de bloqueo total e ir abriendo servicios y puertos necesarios para la ejecución de los servicios. Como parte de las tareas a realizar en el departamento de sistemas se incorpora la revisión de los accesos.

Los sistemas de administración y los sistemas de producción están en entornos separados tal como se indica en el documento de referencia.

Documentación de referencia: IN-2011-04-10 Control de accesos a red.

6.8. Fuentes de Tiempo

Camerfirma tiene un procedimiento de sincronización de tiempo coordinado con el ROA Real Instituto y Observatorio de la Armada en San Fernando vía NTP También obtiene una fuente segura vía GPS y sincronización vía Radio.

Documentación de referencia: IN-2006-04-01-Sincronizacion de tiempos

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. Perfil de Certificado

Los perfiles de certificados cumplen el RFC 5280.

Todos los certificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3 y al RFC 3739 y ETSI 101 867 "Qualified Certificate Profile", pero no pueden ser considerados certificados cualificados conforme al Reglamento eIDAS al no haber sido objeto de una Evaluación de Conformidad

Los perfiles de dichos certificados se pueden solicitar al correo gestion_soporte@camerfirma.com o al teléfono 902 361 207

7.1.1 Número de versión

Camerfirma emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Los documentos de las extensiones de los certificados se encuentran detallados en las fichas de perfiles. Las fichas de perfiles se pueden solicitar en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es
- 1.2.840.113549.1.1.5 - sha1withRSAEncryption
- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption

El campo *Subject Public Key Info* (1.2.840.113549.1.1.1) incorpora el valor *rsaEncryption*

7.1.4 Formato de Nombres.

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica.

En general, los certificados de uso en el sector público deberán contener la identidad de la persona que los recibe, preferiblemente en los campos Subject Name o Subject Alternative Name, incluyendo los siguientes datos:

- Nombre y apellidos de la persona Firmante, poseedora o representada, en campos separados, o con indicación del algoritmo que permite la separación de forma automática.
- Denominación social de la persona jurídica, cuando corresponda.
- Números de documentos de identificación correspondientes, de acuerdo con la legislación aplicable a la persona Firmante, poseedora o representada, sea física o jurídica.

Esta norma no se aplica a los certificados con seudónimo, que deben identificar esta condición.

La semántica exacta de los nombres se describe en las fichas de los perfiles. Las fichas de perfiles se pueden solicitar en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207

7.1.5 Restricciones de los nombres

Camerfirma puede utilizar restricciones de nombre (utilizando la extensión del certificado "name constrains") en aquellos certificados de AC subordinada emitidos a terceras partes de forma que solo se pueda emitir por la AC subordinada el conjunto de certificados permitido en dicha extensión.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

Todos los certificados Camerfirma tienen un identificador de política que comienza desde la base 1.3.6.1.4.1.17326.

Govern d'Andorra = 2.16.20.2.1.3.1

7.1.7 Uso de la extensión "Policy Constraints"

Camerfirma puede utilizar restricciones de política (utilizando la extensión del certificado "*policy constrains*") en aquellos certificados de AC subordinada emitidos a terceras partes de forma que solo se pueda emitir por la AC subordinada el conjunto de certificados permitido en dicha extensión.

7.1.8 Sintaxis y semántica de los calificadores de política

No estipulado

7.1.9 Tratamiento semántico para la extensión critica "*Certificate Policy*"

La extensión "*Certificate Policy*" identifica la política que define las prácticas que Camerfirma asocia explícitamente con el certificado. La extensión puede contener un calificador de la política. Ver 7.1.6.

7.2. Perfil de CRL

El perfil de las CRLs se corresponde con el propuesto en las Políticas de certificación correspondientes. Las CRLs son firmadas por la AC que ha emitido los certificados.

El perfil detallado de la CRL se puede solicitar en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207.

7.2.1 Número de versión

Las CRL emitidas por Camerfirma son de la versión 2.

7.2.2 CRL y extensiones

Las impuestas por las políticas de certificación correspondientes. El perfil detallado de la CRL y sus extensiones se puede solicitar en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207.

7.3. Perfil de OCSP

7.3.1 Número de versión

Los certificados de respondedor OCSP son versión 3. Estos certificados son emitidos por cada AC gestionada por AC Camerfirma según el estándar RFC 6960.

7.3.2 Extensiones OCSP

Se puede obtener el perfil de los certificados respondedores de OCSP en el siguiente correo gestion_soporte@camerfirma.com o al teléfono 902 361 207.

Se puede obtener una lista actualizada de los certificados de OCSP en http://www.camerfirma.com/servicios/respondedor-ocsp.

8. AUDITORÍAS DE CONFORMIDAD

Camerfirma es una empresa comprometida con la seguridad y la calidad de sus servicios.

Los objetivos de Camerfirma respecto a la seguridad y la calidad han sido fundamentalmente la obtención de la certificación ISO/IEC 27001, ISO/IEC 20000 y la realización de Auditorías internas bienales al Sistema de certificación Camerfirma, y fundamentalmente a las Autoridades de registro, para garantizar el cumplimiento de los procedimientos internos.

Camerfirma está también sujeta a los controles que realiza el organismo regulador nacional respecto a su actividad, siendo este el Ministerio de Industria del Gobierno de España.

Las Autoridades de Registros pertenecientes a ambas jerarquías están sujetas a un proceso de auditoría interna. Estas auditorías se realizan periódicamente de forma discrecional en base a una valoración de riesgo por el número de certificados emitidos y número de operadores de registro, lo que determinará también que se realice la auditoria de forma presencial o remota. Las auditorias se describen en un "Plan Anual de Auditorias".

AC Camerfirma está sujeta a una auditoria bienal sobre LOPD/RGPD.

AC Camerfirma realiza una auditoria interna a aquellas entidades que hayan obtenido un certificado de AC subordinada o TSU y que emitan y gestionen certificados con sus propios recursos técnicos y operativos. En esta auditoria Camerfirma comprueba de forma aleatoria un número de certificados emitidos por dicha autoridad de registro, asegurándose de que las evidencias recogidas sean correctas y suficientes para la emisión del certificado.

8.1. Frecuencia o circunstancias de las auditorias

Como se ha indicado en el apartado 2.7, Camerfirma lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza de forma discrecional

- Auditoria ISO 27001, ISO20000, ISO 9001, ciclo de 3 años con revisiones anuales.
- .
- Evaluación de conformidad eIDAS, bienal con revisión anual (para CAs cualificadas)
- Auditoria LOPD/RGPD, bienal con revisión anual.
- Un análisis de vulnerabilidades trimestral
- Un análisis de intrusión anual.
- Auditorías de RA de forma discrecional.
- TSU Externas, de forma discrecional.

8.1.1 Auditorías de AC subordinada Externa o certificación cruzada.

AC Camerfirma a través de sus auditores realiza una auditoria anual a las organizaciones que han obtenido un certificado de SubCA o TSA y que emiten certificados con sus propios medios técnicos y operativos. Esta auditoria puede ser sustituida por un certificado favorable de auditoria *Webtrust BR, WebTrust for CA* y/o *WebTrust for EV* según corresponda a los certificados emitidos.

8.1.2 Auditoria en las Autoridades de Registro

Todas las AR son auditadas. Estas auditorías se realizan al menos cada dos años de forma discrecional y en base a un análisis de riesgos. Las auditorias comprueban el cumplimiento de los requerimientos exigidos por las Políticas de Certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado.

Dentro de la auditoría interna realizada se toman muestreos sobre certificados emitidos, verificando su correcto procesamiento.

Documentación de referencia respecto a los procesos de auditoria de las AR son:
- IN-2010-04-12-Procedimiento de Evaluación de la Seguridad en AR
- IN-2010-04-15-Ficha de la visita de evaluación.doc
- IN-2010-04-16-Lista de Chequeo
- IN-2006-03-08-Procedimiento Labores de AR.
- IN-2010-04-17-Informe de evaluación

8.1.3 Auditorías Internas

Adicionalmente a las auditorias definidas previamente, AC Camerfirma realiza internamente controles de calidad sobre el 3% de los certificados de servidor emitidos. El periodo de auditorías comienza inmediatamente después de que se tomó la última muestra.

La auditoría consiste en la revisión de la veracidad y soporte documental de los datos incorporados en el certificado seleccionado en la muestra.

El departamento encargado realizará un acta sobre la auditoría realizada.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por las compañías independientes externas siguientes de amplio reconocimiento en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación:
- Para las auditorías ISO27001/20000 ISO 9001 -CSQA. http://www.csqa.it
- Para las auditorías internas / RA / AC subordinada, TSA LOPD/RGPD – AUREN http://www.auren.com/

8.3. Relación entre el auditor y la AC

Las empresas de auditoría son independientes y de reconocido prestigio contando con departamentos especializados en la realización de auditorías informáticas en la gestión de certificados digitales y servicios de confianza, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la AC.

No existe vinculación ni dependencia financiera ni orgánica entre las empresas auditoras y AC Camerfirma.

8.4. Tópicos cubiertos por la auditoria

En líneas generales, las auditorías verifican:

a) Que Camerfirma tiene un sistema que garantiza la calidad del servicio prestado.
b) Que la CPS, se ajusta a lo establecido en las Políticas, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.
c) Que Camerfirma gestiona de forma adecuada la seguridad de sus sistemas de información.
d) En los certificados la auditoría comprueba la alienación con las políticas marcadas por CABFORUM en las "Baseline Requirement".

En líneas generales, los elementos objeto de auditoría serán los siguientes:

- Procesos de Camerfirma, ARs y elementos relacionados en la emisión de certificados y servicios de validación en línea OCSP.
- Sistemas de información.
- Protección del centro de proceso de datos.
- Documentación requerida para cada tipo de certificado.
- Verificación de que los operadores de RA conocen la CPS y Políticas de AC Camerfirma

8.5. Acciones tomadas como resultado de las deficiencias

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, Camerfirma discutirá, con la entidad que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo con objeto de solucionar las deficiencias.

Si la Entidad auditada es incapaz de desarrollar y / o ejecutar dicho plan en el plazo de tiempo solicitado, o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicar inmediatamente la autoridad de políticas, que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar el certificado correspondiente, y regenerar la infraestructura.
- Terminar el servicio a la Entidad.
- Otras acciones complementarias que resulten necesarias.

8.6. Comunicación de resultados

La comunicación de resultados ser realiza al responsable de seguridad y cumplimiento normativo por parte de los auditores que han realizado la evaluación. Se realiza en un acto con

presencia de la dirección corporativa. El certificado de auditoria se publica en la Web de Camerfirma.

9. ASPECTOS LEGALES Y OTROS ASUNTOS

9.1. Tarifas

9.1.1 Tarifas de emisión de certificados y renovación.

Los precios de los servicios de certificación o cualquier otro servicio relacionado están disponibles y actualizados en la página Web de Camerfirma http://www.camerfirma.com/certificados/ o previa consulta al departamento de soporte de Camerfirma en https://secure.camerfirma.com/incidencias/ o al teléfono 902 361 207.

Cada tipo de certificado tiene publicado su precio concreto, excepto aquellos que están sujetos a una negociación comercial previa.

9.1.2 Tarifas de acceso a los certificados.

El acceso a los certificados emitidos es gratuito. AC Camerfirma implementa controles para evitar los casos de descarga masiva de certificados. Cualquier otra circunstancia que a juicio de Camerfirma deba ser considerada a este respecto se publicara en la página Web de Camerfirma https://www.camerfirma.com/noticias/ o previa consulta al departamento de soporte de Camerfirma en https://www.camerfirma.com/ayuda/soporte/ o al teléfono 902 361 207.

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

Camerfirma provee un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito a través de listas de certificados revocados o mediante acceso vía Web en la dirección Internet de Camerfirma https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.
Camerfirma ofrece el servicio de OCSP de forma gratuita.
https://www.camerfirma.com/servicios/respondedor-ocsp/.

9.1.4 Tarifas por el acceso al contenido de estas Prácticas de certificación.

El acceso al contenido de la presente CPS es gratuito, en la dirección Web de Camerfirma https://policy.camerfirma.com.

9.1.5 Política de reintegros.

AC Camerfirma no tiene una política de reintegros específica, y se acoge a la normativa general vigente.
La emisión correcta del certificado digital sea en el soporte que sea, supone el comienzo de la ejecución del contrato, con lo que, conforme lo permite la Ley General para la Defensa de los Consumidores y Usuarios (RDL 1/2007) en dichos casos, el Sujeto/Titular pierde su derecho de desistimiento.

9.2. Responsabilidad financiera

9.2.1 Cobertura del Seguro

Camerfirma, en su actividad como PSC, dispone de un seguro de responsabilidad civil que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios: el Sujeto/Firmante y la Parte Usuaria y a terceros, por un importe conjunto de 3.700.000 de euros.

9.2.2 Otros activos

No estipulado.

9.2.3 Seguro de cobertura o garantía para entidades finales

Ver apartado 9.2.1

9.3. Confidencialidad de la información del negocio

9.3.1 Tipo de información a mantener confidencial

Camerfirma considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

Camerfirma dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

Documentación de referencia:
- IN-2005-02-04-Política de Seguridad.
- IN-2006-02-03-Normativa Seguridad.

9.3.2 Tipo de información considerada no confidencial

Camerfirma considera como información no confidencial:

a) La contenida en la presente CPS y en las Políticas de Certificación
b) La información contenida en los certificados.
c) Cualquier información cuya accesibilidad sea prohibida por la normativa vigente.

9.3.3 Responsabilidad de proteger la información confidencial

Camerfirma es responsable de la protección de la información confidencial generada o comunicada durante todas las operaciones. Las partes delegadas, como las entidades que

administran las CA emisoras subordinadas o las autoridades de registro, son responsables de proteger la información confidencial que se ha generado o almacenado por sus propios medios. Para las entidades finales, los suscriptores del certificado son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesaria para acceder o usar la clave privada.

9.3.3.1 Divulgación de información de revocación / suspensión de certificados

Camerfirma difunde la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRLs.

Camerfirma dispone de un servicio de consulta de CRL y Certificados en el sitio de Internet: http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Camerfirma dispone de un servicio de consulta online de estado de los certificados basado en el estándar OCSP en la dirección http://ocsp.camerfrima.com. El servicio OCSP ofrece respuestas estandarizadas bajo el RFC 2560 sobre el estado de un certificado digital, es decir, si el certificado consultado está activo, revocado o si ha sido emitido o no por la autoridad de certificación.

La política de difusión de información de revocación de certificados en AC subordinadas Externas con uso de tecnología propia, se realizará en base a sus propias CPS.

9.3.3.2 Envío a la Autoridad Competente

Camerfirma proporcionará la información solicitada por la autoridad competente o al organismo regulador correspondiente, en los casos y forma establecidos en la legislación vigente.

9.4. Privacidad de la información personal

9.4.1 Plan de privacidad

Camerfirma cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos, en particular, ha adaptado sus procedimientos al REGLAMENTO (UE) 2016/679 General de Protección de Datos (RGPD). En este sentido, este documento sirve, de conformidad con la Ley 59/2003, de Firma Electrónica (artículo 19.3) y el Reglamento eIDAS (artículo 24.2.f) como documento de seguridad.

Documentación de referencia: IN-2006-05-11-Conformidad de Requerimientos legales

9.4.2 Información tratada como privada

La información personal sobre un individuo que no está públicamente disponible en los contenidos de un certificado o CRL se considera privada.

9.4.3 Información no considerada privada

La información personal sobre un individuo disponible en los contenidos de un certificado o CRL, se considera como no privada al ser necesaria a la prestación del servicio contratado, sin

perjuicio de los derechos correspondientes al titular de los datos personales en virtud de la legislación LOPD/RGPD.

9.4.4 Responsabilidad de proteger la información privada

Es responsabilidad del responsable del tratamiento proteger adecuadamente la información privada.

9.4.5 Aviso y consentimiento para usar información privada

Antes de entablar una relación contractual, Camerfirma ofrecerá a los interesados la información previa acerca del tratamiento de sus datos personales y ejercicio de derechos, y en su caso, recabará el consentimiento preceptivo para el tratamiento diferenciado del tratamiento principal para la prestación de los servicios contratados.

9.4.6 Divulgación de conformidad con un proceso judicial o administrativo

Los datos personales que sean considerado privados o no, solo podrán divulgarse en caso cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

9.4.7 Otras circunstancias de divulgación de información

No se cederán datos personales a terceros salvo obligación legal.

9.5. Derechos de propiedad intelectual

Camerfirma es titular de los derechos de propiedad intelectual sobre esta CPS. La CPS de las AC subordinadas ligadas a las jerarquías de Camerfirma es titularidad de Camerfirma, sin perjuicio de las cesiones de uso de sus derechos a favor de las AC subordinadas y sin perjuicio de las aportaciones de las propias AC subordinadas que son titularidad de éstas.

9.6. Obligaciones y Responsabilidad Civil

9.6.1 Obligación y responsabilidad de la CA

9.6.1.1 AC

Camerfirma se obliga según lo dispuesto en las Políticas de Certificación implicadas y en esta CPS, así como lo dispuesto en normativa vigente sobre prestación de servicios de Certificación a:

- Respetar lo dispuesto en el alcance de esta CPS y en las Políticas de Certificación correspondientes.
- Proteger sus claves privadas de forma segura.
- Emitir certificados conforme a esta CPS, a las Políticas de Certificación y a los estándares técnicos de aplicación.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados no cualificados.
- Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- Suspender y revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL.
- Informar a los Sujetos/Firmantes de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación vigente.
- Publicar esta CPS y las Políticas de Certificación correspondientes en su página Web.
- Informar sobre las modificaciones de esta CPS y de las Políticas de Certificación a los Sujetos/Firmantes y a las RAs que estén vinculadas a ella.
- No almacenar ni copiar los datos de creación de firma del Sujeto/Firmante excepto para los certificados de cifrado y para los casos en los que legalmente se prevea o permita dicho almacenaje o copia.
- Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia, en su caso.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida o destrucción o falsificación.
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

Para los certificados emitidos en dispositivo centralizado (CKC), custodiar con la debida diligencia las claves privadas de los certificados La responsabilidad de Camerfirma

El artículo 22.1 de la Ley de Firma Electrónica establece que:

"Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que impone esta Ley.

La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

Así pues, Camerfirma será responsable de los daños y perjuicios ocasionados a los usuarios por sus servicios, ya sea al Firmante/Suscriptor o al Tercero que confía, y a otros terceros en los términos establecidos en la legislación vigente y en las Políticas de Certificación.

En este sentido Camerfirma es la única responsable (i) de la emisión de los certificados, (ii) de su gestión durante todo el ciclo de vida de éstos y (iii) en particular, si es preciso, en caso de suspensión y revocación de los certificados. En concreto, Camerfirma fundamentalmente será responsable de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión, mediante la confirmación de los datos del solicitante y las prácticas de AR.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Firmante/Suscriptor, la clave privada correspondiente a la clave pública dada o identificada en el certificado cuando el proceso así lo requiera, mediante la utilización de peticiones estandarizadas en formato PKCS#10.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente, utilizando dispositivos y mecanismos criptográficos certificados.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

En cumplimiento de la legislación vigente Camerfirma dispone de un seguro de responsabilidad civil que cubre los requerimientos marcados por las políticas de certificación afectadas por estas prácticas de certificación.

9.6.1.2 CA Subordinada Externa

Las CAs subordinadas externas son CA incorporadas a la jerarquía de la AC raíz pero son propiedad de una organización distinta y pueden usar o no una infraestructura técnica distinta.

- Proteger sus claves privadas.
- Emitir certificados conforme a las políticas de certificación y/o CPS correspondiente.
- Emitir certificados libres de errores
- Publicar los certificados en un repositorio accesible por AC Camerfirma.
- Permitir la auditoria anual.
- Custodiar durante el tiempo marcado por la legislación vigente de la información documental y de los sistemas que se han servido o generado para la emisión de los certificados.
- Notificar a AC Camerfirma de cualquier incidencia en la actividad delegada.

Responsabilidad de la SubCA (Interna/Externa).

Sin perjuicio de la responsabilidad de Camerfirma por la emisión y revocación de los certificados digitales de las propias SubCAs así como de los términos contractuales acordados en cada caso, éstas (a través de la entidad con personalidad jurídica de la que dependen) serán responsables de la emisión y revocación de los certificados digitales emitidos a usuario final, respondiendo ante los suscriptores y demás terceros o usuarios afectados por el servicio de acuerdo con sus propias Declaraciones de Practicas de Certificación, Políticas de Certificación y su legislación nacional en su caso.

9.6.2 Obligación y responsabilidad de la RA

Las AR son las entidades delegadas por la AC para realizar las tareas de registro y aprobación de las solicitudes de certificados, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

- Respetar lo dispuesto en esta CPS y en la Política de Certificación correspondiente.
- Proteger sus claves privadas que les servirán para el ejercicio de sus funciones.
- Comprobar la identidad de los Sujetos/Firmantes y Solicitantes de los certificados cuando resulte necesario, acreditando definitivamente la identidad del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización, de acuerdo con lo establecido en las secciones correspondientes de este documento.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- Proporcionar al Firmante, en caso de certificados individuales, o al futuro poseedor de claves, en caso de certificados de organización, acceso al certificado.
- Entregar, en su caso, el dispositivo criptográfico correspondiente.
- Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o Firmante.
- Respetar lo dispuesto en los contratos firmados con Camerfirma y con el Sujeto/Firmante.
- Informar a Camerfirma de las causas de revocación, siempre y cuando tomen conocimiento.
- Ofrecer información básica sobre la política y uso del certificado, incluyendo especialmente información sobre Camerfirma y la Declaración de Prácticas de Certificación aplicable, así como de sus obligaciones, facultades y responsabilidades.
- Ofrecer Información sobre el certificado y el dispositivo criptográfico.
- Recopilar información y evidencias del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de dichos elementos.
- Informar del método de imputación exclusiva al poseedor de la clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones correspondientes de este documento.

Estas obligaciones se aplican incluso en los casos de entidades delegadas por estas como son los puntos de verificación presencial (PVP).

La información sobre el uso y responsabilidades de suscriptor se suministra mediante la aceptación de las cláusulas de uso previamente a la confirmación de la solicitud del certificado y mediante correo electrónico.

La responsabilidad de las RA

Las RA suscriben un contrato de prestación de servicio con Camerfirma mediante el cual Camerfirma delega las funciones de registro en las RA, consistente fundamentalmente en:

1.- Obligaciones previas a la expedición de un certificado.

a) Informar adecuadamente a los solicitantes de la firma de sus obligaciones y responsabilidades.
b) La adecuada identificación de los solicitantes, que deben ser personas capacitadas o autorizadas para solicitar un certificado digital.
c) La correcta comprobación de la validez y vigencia de esos datos de los solicitantes y de la Entidad, en el caso de que exista una relación de vinculación ó representación.
d) Acceder a la aplicación de Autoridad de Registro para gestionar las solicitudes y los certificados emitidos.

2.- Obligaciones una vez expedido el certificado.

a) Suscribir los contratos de Prestación de Servicios de Certificación Digital con los solicitantes. En la mayoría de los procesos de emisiones este contrato es formalizado mediante la aceptación de condiciones en las páginas web que forman parte del proceso de emisión del certificado, no pudiéndose realizar la emisión sin antes no haber aceptado las condiciones de uso.
b) El mantenimiento de los certificados durante su vigencia (extinción, suspensión, revocación).
c) Archivar las copias de la documentación presentada y los contratos debidamente firmados por los solicitantes en conformidad con Políticas de Certificación publicadas por Camerfirma y la legislación vigente.

Así pues, las RA se responsabilizan de las consecuencias en caso de incumplimiento de sus labores de registro, y a través del cual se comprometen a respetar además las normas reguladoras internas de la entidad certificadora Camerfirma (Políticas y CPS) las cuales deberán ser perfectamente controladas por parte de las RA y que deberán servirles de manual de referencia.

En caso de reclamación por un Sujeto, una Entidad, o un usuario, la AC deberá aportar la prueba de la actuación diligente y si se constata que el origen de la reclamación radica en un error en la validación o comprobación de los datos, la AC podrá en virtud de los acuerdos firmados con las RA, hacer soportar a la RA responsable la asunción de las consecuencias. Porque, aunque legalmente sea la AC la persona jurídica responsable frente al Sujeto, una Entidad, o Parte Usuaria, y que para ello dispone de un seguro de responsabilidad civil, según el acuerdo vigente y las Políticas vinculantes, la RA tiene como obligación contractual "identificar y autenticar correctamente al Solicitante y, en su caso, a la Entidad que corresponda", y en su virtud deberá responder frente a Camerfirma de sus incumplimientos.

Por supuesto, no es intención de Camerfirma descargar todo el peso de la asunción de responsabilidad a las RA en cuanto a los posibles daños cuyo origen vendría de un incumplimiento de las tareas delegadas a las RA. Por esta razón, al igual que lo previsto para la AC, la RA se ve sometida a un régimen de control que será ejercido por Camerfirma, no solamente a través de los controles de archivos y procedimientos de conservación de los archivos asumidos por la RA mediante la realización de auditorías para evaluar entre otros, los recursos empleados y el conocimiento y control de los procedimientos operativos para ofrecer los servicios de RA.

Las mismas responsabilidades deberá asumir las RA en virtud de incumplimientos de las entidades delegadas como por ejemplo los puntos de verificación presencial (PVP), sin perjuicio de su derecho a repercutir contra ellas.

9.6.3 Obligación y responsabilidad del suscriptor

9.6.3.1 Firmante/Suscriptor

El Firmante/Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Usar el certificado según lo establecido en la presente CPS y en las Políticas de Certificación aplicables.
- Respetar lo dispuesto en los documentos firmados con Camerfirma y la AR.
- Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión /revocación.
- Notificar cualquier inexactitud o cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por Camerfirma o la AR de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.
- Hacer uso del certificado digital con el carácter de personal e intransferible y, por tanto, asumir la responsabilidad por cualquier actuación que se lleve a cabo en contravención de esta obligación, así como cumplir las obligaciones que sean específicas de la normativa aplicable a las dichas certificaciones digitales.
- Autorizar a Camerfirma proceder al tratamiento de los datos personales contenidos en los certificados, en conexión con las finalidades de la relación electrónica y, en todo caso, para cumplir las obligaciones legales de verificación de certificados.
- Responsabilizarse de que toda la información incluida, por cualquier medio, la solicitud del certificado y en el mismo certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.
- Informar inmediatamente al prestador de servicios de certificación correspondiente, de cualquier inexactitud en el certificado detectada una vez se haya emitido, así como de los cambios que se produzcan en la información aportada por la emisión del certificado.
- Si se trata de certificados en un dispositivo material, en caso de que pierda su posesión, ponerlo en conocimiento fehaciente de la entidad que lo haya emitido en el plazo más breve posible y, en todo caso, dentro de las 24 horas siguientes a la producción de la mencionada circunstancia, con independencia del hecho concreto que la haya originado o de las acciones que eventualmente pueda ejercer.
- No utilizar la clave privada, el certificado electrónico o cualquier otro soporte técnico entregado por el prestador de servicios de certificación correspondiente para realizar ninguna transacción prohibida por la ley aplicable.

En el caso de certificados calificados, el suscriptor o el poseedor de certificados debe utilizar el par de claves exclusivamente para la creación de firmas o sellos electrónicos y de acuerdo con cualesquiera otras limitaciones que le sean notificadas.

Asimismo, debe ser especialmente diligente en la custodia de su clave privada y de su dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados. Será el único responsable frente a terceros o frente a la entidad que representa si no está autorizado para ello, de las consecuencias que un uso indebido o no correctamente controlado pueda generar.

Si el suscriptor genera sus propias claves, se obliga a:

- Generar sus claves de suscriptor utilizando un algoritmo reconocido como aceptable para la firma electrónica, , o el sello electrónico.
- Crear las claves dentro del dispositivo de creación de firma o de sello, utilizando un dispositivo seguro cuando proceda.
- Utilizar longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica, , o el sello electrónico.

9.6.3.2 Solicitante del certificado

El Solicitante (bien directamente o a través de un tercero autorizado) de un certificado estará obligado a cumplir con lo dispuesto por la normativa y además a:

- Suministrar a la AR la información necesaria para realizar una correcta identificación.
- Garantizar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Custodiar su clave privada de manera diligente.

9.6.3.3 Entidad

En el caso de aquellos certificados que impliquen vinculación a una Entidad, la Entidad vendrá obligada a solicitar a la RA la suspensión/revocación del certificado cuando el Sujeto/Firmante cese dicha vinculación respecto a la organización.

9.6.4 Obligación y responsabilidad de terceras partes

Será obligación de la Parte Usuaria cumplir con lo dispuesto por lo dispuesto en la normativa vigente y, además:

- Verificar la validez de los certificados antes de realizar cualquier operación basada en los mismos. Camerfirma dispone de diversos mecanismos para realizar dicha comprobación como el acceso a listas de revocados o a servicios de consulta en línea como OCSP, todos estos mecanismos están descritos en la página Web de Camerfirma.
- 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. En los certificados de Representante de Persona Jurídica (o entidad sin personalidad jurídica) para Apoderados que implican una relación de representación basada en un poder especial notarial o documento privado con facultades limitadas, las terceras partes deberán comprobar los límites de dichas facultades.
- Comprobar la validez de la cualificación de una firma asociada a un certificado emitido por Camerfirma comprobando que la autoridad de certificación que ha emitido el certificado se encuentra publicada en la lista de confianza del supervisor nacional correspondiente.

9.6.5 Obligación y responsabilidad de otras participantes

No estipulado

9.7. Exoneración de responsabilidad

Según la legislación vigente, la responsabilidad de CAMERFIRMA y de la RA no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Sujeto, y a la Parte Usuaria por:

- No haber proporcionado información adecuada, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado electrónico, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación;
- Haber incurrido en negligencia con respecto a la conservación de los datos de creación de firma y a su confidencialidad;
- No haber solicitado la suspensión o revocación de los datos del certificado electrónico en caso de duda sobre el mantenimiento de la confidencialidad;
- Haber utilizado la firma después de haber expirado el periodo de validez del certificado electrónico;
- Superar los límites que figuren en el certificado electrónico.
- En conductas imputables a la Parte Usuaria si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado
- De los daños ocasionados al Sujeto o terceros que confía por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible.

- Un uso inadecuado o fraudulento del certificado en caso de que el Sujeto/Titular lo haya cedido o haya autorizado su uso a favor de una tercera persona en virtud de un negocio jurídico como el mandato o apoderamiento, siendo exclusiva responsabilidad del Sujeto /Titular el control de las claves asociadas a su certificado.

Camerfirma y las RAs tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en las Políticas de Certificación
- Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la AC
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Sujeto.

9.8. Limitación de responsabilidad en caso de pérdidas por transacciones

El límite monetario del valor de las transacciones se expresa en el propio certificado de entidad final mediante la inclusión de una extensión "*qcStatements*", (OID 1.3.6.1.5.5.7.1.3), tal como se define en la RFC 3039. La expresión del valor monetario se ajustará a lo dispuesto en la sección 5.2.2 de la norma TS 101 862 de la ETSI (*European Telecommunications Standards Institute*, www.etsi.org).

Si la extensión del certificado anteriormente expuesta no lo contradice, el límite máximo que Camerfirma permite en las transacciones económicas realizadas es de 0 (cero) euros.

9.9. Indemnizaciones

Ver apartado 9.2

9.10. Plazo y Finalización

9.10.1 Plazo

Ver apartado 5.8

9.10.2 Terminación

Ver apartado 5.8

9.10.3 Efecto de la terminación y la supervivencia

Ver apartado 5.8

9.11. Notificaciones individuales y comunicación con los participantes

Cualquier notificación referente a la presente CPS se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto 1.5.2.

9.12. Modificaciones

9.12.1 Procedimiento de modificación.

La CA se reserva el derecho de modificar este documento por razones técnicas o para reflejar cualquier cambio en los procedimientos que se hayan producido debido a requisitos legales, reglamentarios (eIDAS, CA/B Forum, Organismos de Supervisión Nacional, etc.) o como

resultado de la optimización del ciclo de trabajo. Cada nueva versión de esta CPS reemplaza a todas las versiones anteriores, que siguen siendo, sin embargo, aplicables a los certificados emitidos mientras esas versiones estaban vigentes y hasta la primera fecha de vencimiento de esos certificados. Se publicará al menos una actualización anual. Estas actualizaciones quedaran reflejadas en el cuadro de versiones al inicio del documento.

Los cambios que pueden realizarse a esta CPS no requieren notificación excepto que afecte de forma directa a los derechos de los Sujetos/Firmantes de los certificados, en cuyo caso podrán presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

9.12.2 Mecanismo de notificación y plazos

9.12.2.1 Lista de elementos

Cualquier elemento de esta CPS puede ser cambiado sin preaviso.

9.12.2.2 Mecanismo de notificación

Todos los cambios propuestos de esta política serán inmediatamente publicados en la Web del Camerfirma

https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

En este mismo documento existe un apartado de cambios y versiones donde se puede conocer los cambios producidos desde su creación y la fecha de dichas modificaciones.

Los cambios de este documento se comunican a aquellos organismos y empresas terceras que emiten certificados bajo esta CPS así como a los auditores correspondientes. Especialmente se notificarán los cambios en esta CPS a los organismos de Supervisión Nacional:

- España: Ministerio de Economía y Empresa o aquel en que en ese momento recaiga la supervisión de los prestadores de servicios de confianza.

9.12.2.3 Periodo de comentarios

Los Firmantes/Suscritores y Terceros que confían, afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los **15 días** siguientes a la recepción de la notificación. Las Políticas dicen que 15 días

9.12.2.4 Mecanismo de tratamiento de los comentarios

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

9.12.3 Circunstancias en las que se debe cambiar el OID

No estipulado

9.13. Procedimiento de resolución de conflictos

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.

9.14. Legislación aplicable

La ejecución, interpretación, modificación o validez de la presente CPS se regirá por lo dispuesto en la legislación española y de la Unión Europea vigente en cada momento.

9.15. Conformidad con la Ley Aplicable

Ver punto 9.14

9.16. Otras disposiciones

9.16.1 Acuerdo completo

Los Titulares y terceros que confían en los Certificados asumen en su totalidad el contenido de la presente Declaración de Prácticas y Políticas de Certificación.

9.16.2 Asignación

Las partes de esta CPS no pueden ceder ninguno de sus derechos u obligaciones bajo esta CPS o acuerdos aplicables sin el consentimiento por escrito de Camerfirma.

9.16.3 Separabilidad

Si las disposiciones individuales de esta CPS resultan ineficaces o incompletas, esto se hará sin perjuicio de la efectividad de todas las demás disposiciones.

La disposición ineficaz será reemplazada por una disposición efectiva que se considera que refleja más de cerca el sentido y el propósito de la disposición ineficaz. En el caso de disposiciones incompletas, se acordará una modificación que se considere que corresponde a lo que razonablemente se habría acordado de acuerdo con el sentido y los propósitos de esta CPS, si el asunto se hubiera considerado de antemano.

9.16.4 Cumplimiento (honorarios de abogados y exención de derechos)

Camerfirma puede solicitar una indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de dicha parte. El hecho de que

Camerfirma no haga cumplir una disposición de esta CPS no elimina el derecho de Camerfirma de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de esta CPS. Para ser efectiva, cualquier renuncia debe estar por escrito y firmada por Camerfirma.

9.16.5 Fuerza mayor

Las cláusulas de fuerza mayor, si existen, están incluidas en el "Acuerdo del suscriptor".

9.17. Otras provisiones

9.17.1 Publicación y copia de la política

Una copia de esta CPS estará disponible en formato electrónico en la dirección de Internet:

https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/

9.17.2 Procedimientos de aprobación de la CPS

La publicación de las revisiones de esta CPS deberá estar aprobada por la Gerencia de Camerfirma.

AC Camerfirma publica en su página web cada nueva versión. La CPS se publica en formato PDF firmado electrónicamente por la gerencia de AC Camerfirma SA.

ANEXO I: historia del documento

Oct 2004	v2.0	Nuevas Jerarquías. Incorporación de la política de firma de código. Corrección de erratas v2.0
Mar 2004	V2.2	Incorporación de los certificados de apoderado, sello electrónico de empresa y TSA
Jun 2006	V3	Modificación para ajustar el documento a las últimas modificaciones y a la ISO17799. Este documento servirá como documento de seguridad de LOPD y como documento de Seguridad.
May 2007	V3.1	Extinción de certificados Con Poderes y Sin Poderes
Dic 2007	V3.1.1	Revisión de las políticas. (Modificación key usage para incorporar no repudio en los certificados de firma.
May 2008	V3.1.2	Aclaraciones en el proceso de validación de certificados de sello electrónico de empresa y firma de código. Ajustes en los tipos de certificados de la jerarquía RACER con su política de certificación.
Jul 2008	V3.1.3	Incorporación de la AC Corporate Server EV. Ajustes pedidos por el auditor E&Y para auditoria WEBTRUST
Jul 2008	V3.1.4	Incorporación del apartado normativa legal aplicable. Ajustes pedidos por el auditor E&Y para auditoria WEBTRUST
Jun 2009	V3.2	Revisión completa de la redacción, incorporación certificados EV. Incorporación OID RACER. Información de las nuevas claves de ROOT 2008. Certificado de funcionario según desarrollo ley 11/2007 LAECSP. Comentarios validación titular en sello electrónico de empresa. Firma de certificados OCSP por AC. Verificación mensual de los certificados EV.
Feb 2010	V3.2.1	Incorporación de la nueva CA intermedia de AAPP (punto 1.2.1.1 punto 5) Mejora en la descripción del proceso de emisión de certificados EV, exigido por Mozilla. Revisión general. Modificación de la descripción del responsable del certificado (punto 1.4.8 y 2.1.3). Correcciones sobre la emisión de CRL (punto 2.6.2) Correcciones alta AC AAPP (punto 6.1.1) Añadir referencia relativa al HSM nCipher (punto 6.1.8 y 6.2) Modificación 4.8. Modificación en 8.2.1
Feb 2011	V3.2.2	Revisión E&Y proceso de auditoria renovación WebTrust
Mar 2011	V3.2.3	Mejora en la descripción de la definición de la responsabilidad de las distintas partes del sistema de certificación, especialmente, de Camerfirma y de las AR. 2.2. 2.5.5 Política de reintegro 3.1.8 Incorporación de la autorización en los certificados de sello y firma de código. 4.5.4 Eliminación de la revocación por SMS, ya que no se usa. 5.2.2 Validación doble de las peticiones de EV. Modificación de los enlaces a la información en la página web de Camerfirma.
Sep 2011	V3.2.4	Cambio en el perfil del campo 1.3.6.1.4.1.17326.30.3 número de documento identificativo de la organización. Se eliminan los dos primeros caracteres que indican el país, en los perfiles de persona física, representante, apoderado, cifrado y factura electrónica.
Mar 2012	V3.2.5	Revisión Periódica. Mejora de redacción, Incorporación de referencias a documentación técnica externa a este documento. Adaptación BR y EV del CABFORUM Cambio longitud claves de usuario a 2048.

		Incorporación 3.1.4.1
Jun 2015	V3.2.7	Revisión general. Ajustes procedimientos sello de tiempo. Ajustes proceso de emisión SSL. Cambio de direcciones de enlace en la WEB por cambio del gestor de contenidos. Corrección en la tabla de índices. Incorporamos Informa como fuente de información para la emisión de certificados de componente. Incorporamos Autónomos como solicitantes de certificados de componente. Revisión proceso de firma de sello y código. Incorporación del programa de emisión de certificados de SubCA a terceros bien con recursos internos o externos. Incorporamos jerarquía Gobierno de Andorra en ChamberSign Global Root. CGCOM Eliminación del procedimiento obsoleto de certificados para teléfonos móviles Vodafone. (4.3.2.3) Incorporación de aclaraciones sobre la emisión de certificados SAN. 3.1.8.2.1 / 3.1.8.2.5 Incorporación de gestión centralizada de claves en HSM. Correcciones WebTrust 2015.
Sep 2015	V3.2.8	Modificación INDECOPI, Incorporamos como causa de revocación 4.8.2 Causas de revocación: Resolución firma de la autoridad administrativa o judicial competente.
Dic 2015	V3.2.8	Corrección texto 6.2 sobre protección clave privada.
Ene 2016	V3.2.8	Incorporación OID Codesign
Jul 2016	V3.2.9	Sustitución de los certificados de persona Jurídica por certificados de persona física de representación y sello electrónico.
Mar 2018	V3.3	1.2 aclaración sobre el alineamiento de estas prácticas con los Baseline Requirement de CA/B FORUM. 3.1.8.3.1 Incorporación de las comprobaciones CAA en certificados de Servidor Seguro y Sedes electrónicas según RFC 6844. 4.8.3 Revocación por parte de terceros. Revocación en caso de una incorrecta emisión (Requisito CA/BFORUM). 1.5.4 Delegación de validación de dominio. 1.2.1.1 No se emiten certificados de pruebas para SSL/TLS
May 2018	V3.3.1	Adaptación de la estructura del documento DPC en base a la RFC3647. 3.2.3.5 Otros documentos aceptados para acreditar la vinculación entre el titular del dominio y el titular del certificado. 9.1.5 Modificación política de reintegros 9.4 Actualización de la cláusula sobre privacidad de la información personal conforme RGPD 9.7 Exoneración de responsabilidad de la AC y AR en caso de delegación del certificado a un tercero
Sep 2018	V3.3.2	Cambio de orden, denominación y desarrollo en diversos puntos para alinear con RFC3647 Se desarrolla el punto ‘9.12.1 Procedimiento de modificación’
Sep 2018	V3.3.3	3.2.5 Identificación de la vinculación, se declara que la validación de los dominios se realizará por uno de los métodos aceptados por CA/B Forum Declaración de la versión de Guidelines For The Issuance And Management Of Extended Validation Certificates elaborado por el CA/B Forum con las que están alineadas estas CPS
Sep 2018	V3.3.4	Cambios menores en el estilo del documento 3.2.5.1 Identificación de la vinculación. Declaración explicita de los métodos utilizados. 3.2.3 Incorporación del procedimiento de comprobación de control sobre la cuenta de email del solicitante.

		4.2.1 Se incluyen las comprobaciones sobre CAA anteriormente declaradas en 3.2.5.2 3.2.3 actualizado 3.2.5.1 actualizado 9.16.4 actualizado 6.2.3 actualizado
Ago 2019	V3.3.5	Cambios menores en el estilo del documento. 1.1 Actualización de estándares en los que está basada está CPS para ajustarse a su alcance. 1.3.5.2 Actualización para ajustarse a alcance. 1.3.5.4 Incorporación de los perfiles del Govern d'Andorra 1.3.5.9 actualización de alcance 1.3.5.10 Incorporación de certificados del Govern d'Andorra bajo la CA 'RACER' y actualización de alcance. 1.4.1 Usos apropiados de los certificados 2.2.1 Políticas y Prácticas de Certificación. 2.2.2 Términos y condiciones. 3.1.1, 3.3.1, 4.1.2.1, 4.1.2.3 actualización del alcance. 3.1.2 sustitución de nombre de punto 3.1.3 Este punto ya no aplica porque no se emiten certificados de este tipo. 3.1.5.1 Emisión de varios certificados de persona física para un mismo titular 3.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos 3.1.7 Procedimiento de resolución de disputas de nombres 3.2.1 Métodos de prueba de la posesión de la clave privada y referencia a lista de QSCD. 3.2.2.1 Identidad 3.2.3 Identificación de la identidad de un individuo. 3.2.2.5 registro IP url 3.2.5.1 Inclusión de la identificación de certificados del Govern d'Andorra y ajuste de alcance. 3.4 Identificación y autenticación de una solicitud de revocación 4.1.2.4 eliminación referencia políticas 4.1.2.5 Notas certificación cruzada 4.2.2 aclaración entrega documentación y acceso WS 4.2.3 Plazo SubCAs no estipulado 4.3.1.3 Solicitudes WS autenticadas. 4.5.2, 4.6.1, 4.6.3, 4.6.7, 4.8, 4.9, 4.9.1, 4.9.2, 4.9.3, 4.9.6, 4.9.9, 4.9.10, 4.9.13, 4.12.1, 5.1.2, 5.2.1, 5.2.2, 5.3,5.3.7,5.3.8, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.8, 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.7, 5.8, 6.1.1, 6.1.1.1, 6.1.4, 6.2.1.1, 6.2.1.2, 6.2.4, 6.2.5, 6.2.6, 6.2.8, 6.2.9, 6.2.10, 6.2.11, 6.3.2, 6.4.1,6.4.2, 6.6.1, 6.7, 7.1, 7.1.2 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.1.9, 7.2, 7.2.2, 8, 8.1.1, 8.1.3, 8.2, 8.3, 8.4, 9.1.2, 9.1.3, 9.6.1.1, 9.6.2, 9.6.3.1, 9.6.3.2, 9.3.3.3, 9.6.4, 9.9, 9.11, 9.12.2.2, 9.17.1, 9.17.2 actualizaciónes varias para adaptarse a nuevo alcance
Junio 2020	V3.3.6	En todo el documento, se aclara cuando procede que las CAs y los certificados de usuario final son no cualificados por no haber pasado la Evaluación de Conformidad eIDAS. 1.3.5.9 Se añade para mejor información el resto de CAs de la Jerarquía Chambers of Commerce y sus perfiles respectivos 1.3.5.9 (y en el resto del documento donde se haga referencia) se precisa que los perfiles de certificado de "Representante de Entidad con o sin personalidad jurídica para trámites ante las AAPP" dejan de sujetarse a las presentes CPS a contar del 9 de junio de 2020 (pasan bajo regulación de la CPS eIDAS de Camerfirma). 1.3.5.9 (y en el resto del documento donde se haga referencia) se elimina el perfil de Persona Jurídica

		1.3.5.10 Se añade para mejor información el resto de CAs de la Jerarquía Global Chambersign Root aunque sea propiedad de terceras entidades 1.3.5.10 (y en el resto del documento donde se haga referencia) se elimina el perfil de Persona Jurídica 8. Se elimina las referencias a la auditoria WEBTRUST 8.2 Se actualiza el nombre de los auditores