DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA EIDAS-2016

CHAMBERS OF COMMERCE ROOT - 2016 y
GLOBAL CHAMBERSIGN ROOT - 2016.

Versión 1.2.3

FRANCE MARIE SYLVIA VIDAL LECA
Firmado digitalmente por FRANCE MARIE SYLVIA VIDAL LECA
Fecha: 2018.03.28 10:53:01 +02'00'

Elaboración: Juan Ángel Martín: Área PKI.
Luis Miguel Aldea y Eva Vaquero: Área de Sistemas.
Raquel Rodriguez: Área de Operaciones.
France Vidal: Área Jurídica

RAMIRO MUÑOZ MUÑOZ
Firmado digitalmente por RAMIRO MUÑOZ MUÑOZ
Fecha: 2018.03.28 09:15:33 +02'00'

Revisión: Ramiro Muñoz (Dirección Explotación).
Aprobación (PA): France Vidal (Dirección Jurídica).
Auditor: Auren España.

Documento válido solo en formato digital firmado electrónicamente por la Autoridad de Políticas.
Este documento se puede obtener en la dirección https://policy.camerfirma.com/ o solicitándolo por correo a juridico@camerfirma.com ©2017 Camerfirma S.A. Todos los derechos reservados.

Idioma: **Castellano**

Mayo 2016	V1.0	Adaptación EIDAS
Nov 2016	V1.1	Modificaciones realizadas en el proceso de evaluación de conformidad.
Marzo 2017	V1.2	Ampliación de estructuras de CA, revisión y modificaciones perfiles de certificados.
Abril 2017	V1.2.1	3.1.8.2.2 Incorporación de las comprobaciones CAA en certificados de Servidor Seguro y Sedes electrónicas según RFC 6844.
Febrero 2018	V1.2.2	1.2 aclaración sobre el alineamiento de estas prácticas con los Baseline Requirement de CA/B FORUM 1.2.1.3 -Correcciones OIDs de los certificados de EP con PSEUDÓNIMO 1.2.1.3.4 - Aclaración duración de los certificados de TSU y aceptación de las practicas por parte del suscriptor con dispositivo TSU homologado. 1.2.1.4.3 - Incorporación de la fecha de despliegue de Camerfirma Perú 1.5.5 - Incorporación de la figura de Agencia delegada para Camerfirma Perú 4.8.3 Revocación por parte de terceros. Revocación en caso de una incorrecta emisión (Requisito CA/BFORUM)
Marzo 2018	V1.2.3	1.5.5 Las RA para SSL no pueden validar el dominio. CA/B Forum. 2.5.3 Aclaración servicio gratuito OCSP. 2.1.5 responsabilidad usuario - Comprobación TSL

Índice de Contenido

1. Introducción _____ *11*

1.1. Consideración Inicial _____ **11**

1.2. Vista General _____ **11**

1.2.1 Jerarquías _____ 14

1.2.1.1 Emisión de certificados del set de pruebas y certificados de pruebas en general. 14

1.2.1.2 Jerarquía Camerfirma Gestión Interna. _____ 15

1.2.1.3 Jerarquía CHAMBERS OF COMMERCE. _____ 16

1.2.1.3.1 AC CAMERFIRMA FOR WEBSITES. (Certificados para sitios web) 19

1.2.1.3.1.1 Certificados de Website OV (*Organization Validation*) – OVCP. 20

1.2.1.3.1.2 Certificados Cualificados de Website EV (*Extended Validation*) – 20

1.2.1.3.1.3 Certificados Cualificados de Sede electrónica OV y EV - QCP-w. 20

1.2.1.3.2 AC CAMERFIRMA FOR LEGAL PERSONS. (Certificados para personas jurídicas). _____ 20

1.2.1.3.2.1 Certificado Cualificado de Sello Electrónico – QCP-l, QCP-l-qscd. 20

1.2.1.3.2.2 Certificado de Sello Electrónico – LCP. _____ 21

1.2.1.3.2.3 Certificado de Sello Electrónico AAPP. QCP-l, QCP-l-qscd ___ 21

1.2.1.3.3 AC CAMERFIRMA CODESIGN. (Certificados para firma de código). 21

1.2.1.3.3.1 Certificados Cualificados de Firma de Código – QCP-l, QCP-l-qscd. 21

1.2.1.3.3.2 Certificados Cualificados de Firma de Código EV (*Extended Validation*) – QCP-l, QCP-l-qscd. _____ 22

1.2.1.3.4 AC CAMERFIRMA TSA. (Certificados para Sellado de tiempo) 22

1.2.1.3.4.1 Certificado Cualificado de TSU en QSCD _____ 23

1.2.1.3.4.2 Certificado de TSU _____ 23

1.2.1.3.5 AC CAMERFIRMA FOR NATURAL PERSONS. (Certificados para personas físicas) _____ 23

1.2.1.3.5.1 Personas físicas con atributo de vinculación a Entidad. _____ 23

1.2.1.3.5.1.1 Certificado Cualificado Corporativo – QCP-n, QCP-n-qscd.__ 23

1.2.1.3.5.1.2 Certificado Cualificado de Representante Legal: _____ 24

1.2.1.3.5.1.2.1 Certificado Cualificado de Representante de Persona Jurídica con Poderes Generales de Representación. – QCP-n, QCP-n-qscd. _____ 24

1.2.1.3.5.1.2.2 Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica con Poderes Generales de Representación. – QCP-n, QCP-n-qscd. 24

1.2.1.3.5.1.2.3 Certificado Cualificado de Representante Persona Jurídica para trámites con las AAPP. – QCP-n, QCP-n-qscd. _____ 24

1.2.1.3.5.1.2.4 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica para trámites con las AAPP. – QCP-n, QCP-n-qscd. __ 24

1.2.1.3.5.1.2.5 Certificado Cualificado de Representante de Persona Jurídica para Apoderados. – QCP-n, QCP-n-qscd. _____ 24

1.2.1.3.5.1.2.6 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica para Apoderados. – QCP-n, QCP-n-qscd. 25
1.2.1.3.5.1.3 Certificados de Empleado Público. – QCP-n, QCP-n-qscd, NCP+. 25
1.2.1.3.5.2 Personas físicas SIN atributo de vinculación a Entidad. 25
1.2.1.3.5.2.1 Certificado Cualificado de Ciudadano. – QCP-n, QCP-n-qscd. 25
1.2.1.4 Jerarquía GLOBAL CHAMBERSIGN ROOT. 26
1.2.1.4.1 AC CAMERFIRMA. 28
1.2.1.4.1.1 AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS (Certificados para personas físicas) 28
1.2.1.4.1.1.1 Personas físicas CON atributo de vinculación a Entidad. 28
1.2.1.4.1.1.1.1 Certificado Corporativo. 28
1.2.1.4.1.1.1.2 Certificado de Representante de Persona Jurídica. 28
1.2.1.4.1.1.1.3 Certificado de Representante de Entidad sin Personalidad Jurídica. 28
1.2.1.4.1.1.2 Personas físicas SIN atributo de vinculación a Entidad. 29
1.2.1.4.1.1.2.1 Certificado de Ciudadano. 29
1.2.1.4.1.2.1 Certificado de Sello Electrónico. 29
1.2.1.4.2 AC CAMERFIRMA COLOMBIA. 29
1.2.1.4.2.1 AC CITISEG (Certificados para personas físicas y jurídicas) 29
1.2.1.4.3 AC CAMERFIRMA PERÚ. 31
1.2.1.4.3.1 AC CAMERFIRMA PERÚ CERTIFICADOS (Certificados para personas físicas y jurídicas) 31

1.3. Autoridad de Políticas 32

1.4. Identificación 32

1.5. Comunidad y Ámbito de Aplicación. 33
1.5.1 Autoridad de Certificación (AC). 33
1.5.2 Autoridad de Certificación Intermedia o subordinada. 33
1.5.3 Entidad de Acreditación u Organismo de Supervisión. 34
1.5.4 Prestador de servicios de confianza (TSP). 34
1.5.5 Autoridad de Registro (RA) 35
1.5.6 Sujeto/Titular y Firmante. 36
1.5.7 Parte Usuaria o usuario del certificado. 38
1.5.8 Entidad/Organización. 38
1.5.9 Solicitante. 38
1.5.10 Responsable de certificados /Poseedor de las claves 38
1.5.11 Ámbito de Aplicación y Usos. 39
1.5.11.1 Usos Prohibidos y no Autorizados. 39

1.6. Normativa legal aplicable 40

1.7. Contacto 40

2. Cláusulas Generales 41

2.1. Obligaciones 41
2.1.1 AC subordinada externa. 41
2.1.2 RA 42
2.1.3 Firmante 43
2.1.4 Sujeto/Titular. 43
2.1.5 Parte Usuaria/Usuario. 44

2.1.6 Entidad 45
2.1.7 Repositorio 45

2.2. Responsabilidad. 45
2.2.1 Exoneración de responsabilidad 48
2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones 49

2.3. Responsabilidad financiera 49

2.4. Interpretación y ejecución 50
2.4.1 Legislación 50
2.4.2 Independencia 50
2.4.3 Notificación 50
2.4.4 Procedimiento de resolución de disputas. 50

2.5. Tarifas 50
2.5.1 Tarifas de emisión de certificados y renovación. 50
2.5.2 Tarifas de acceso a los certificados. 51
2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados. 51
2.5.4 Tarifas por el acceso al contenido de estas Prácticas de certificación. 51
2.5.5 Política de reintegros. 51

2.6. Publicación y repositorios. 51
2.6.1 Publicación de información de la AC. 51
2.6.1.1 Políticas y Prácticas de Certificación. 52
2.6.1.2 Términos y condiciones. 52
2.6.1.3 Difusión de los certificados. 52
2.6.2 Frecuencia de publicación. 53
2.6.3 Controles de acceso a los repositorios. 53

2.7. Auditorías 53
2.7.1 Frecuencia de las auditorías 54
2.7.2 Identificación y calificación del auditor 55
2.7.3 Relación entre el auditor y la AC 55
2.7.4 Tópicos cubiertos por la auditoria 55
2.7.5 Auditorías de AC subordinada Externa. 56
2.7.6 Auditoria en las Autoridades de Registro 56
2.7.7 Tratamiento de los informes de auditoría 56

2.8. Confidencialidad 57
2.8.1 Tipo de información a mantener confidencial 57
2.8.2 Tipo de información considerada no confidencial 57
2.8.3 Divulgación de información de revocación / suspensión de certificados 57
2.8.4 Envío a la Autoridad Competente 58

2.9. Derechos de propiedad intelectual 58

3. Identificación y Autenticación 59

3.1. Registro inicial 59
3.1.1 Tipos de nombres 59
3.1.2 Pseudónimos 60
3.1.3 Reglas utilizadas para interpretar varios formatos de nombres 60
3.1.4 Unicidad de los nombres 60

3.1.4.1 Emisión de varios certificados de persona física para un mismo titular 60
3.1.5 Procedimiento de resolución de disputas de nombres 60
3.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos 61
3.1.7 Métodos de prueba de la posesión de la clave privada. 61
3.1.8 Autenticación de la identidad de un individuo, la entidad y su vinculación. 61
3.1.8.1 En los certificados para operador de RA (Persona Física). 62
3.1.8.2 En los Certificados cualificados. 62
3.1.8.2.1 Identificación del Sujeto/Firmante. 62
3.1.8.2.2 Identidad del servicio o máquina 62
3.1.8.2.3 Identificación de la entidad. 63
3.1.8.2.4 Identificación de la vinculación. 64
3.1.8.3 Consideraciones en la identificación usuario en casos de alto cargo. 67
3.1.8.4 Consideraciones en la identificación usuarios y vinculación en al AAPP. 67
3.1.8.5 Consideraciones especiales para la emisión de certificados fuera de territorio español. 67

3.2. Renovación de la clave 68

3.3. Reemisión después de una revocación 69

3.4. Renovación de certificados sin renovación de claves 70

3.5. Renovación de certificados con renovación de claves 70

3.6. Modificación de certificados 70

3.7. Solicitud de revocación 70

4. Requerimientos Operacionales 71

4.1. Solicitud de certificados 71
4.1.1 Formularios Web. 71
4.1.2 Lotes. 71
4.1.3 Solicitudes de certificados de entidad final en HSM, TSU y AC subordinada. 72
4.1.4 Solicitudes vía capa de *Web Services* (WS). 72
4.1.5 Procesamiento de la solicitud de certificación 73

4.2. Petición de certificación cruzada. 73

4.3. Emisión de certificados 74
4.3.1 Certificados en Software: 74
4.3.2 Certificados en HW (Dispositivo Seguro de Creación de Firma): 75
4.3.2.1 En Tarjeta o Token Criptográfico. 75
4.3.2.2 Peticiones vía WS: 76
4.3.3 Certificado de servidor seguro EV 76
4.3.4 Certificado de cifrado. 77
4.3.5 Certificados de AC subordinada: 77
4.3.6 Certificados de TSU: 77

4.4. Aceptación de certificados. 77

4.5. Notificación de la emisión a los interesados 77

4.6. Publicación del certificado 77

4.7. Notificación de la emisión a terceros 78

4.8. Suspensión y revocación de certificados. 78

4.8.1 Aclaraciones previas 78
4.8.2 Causas de revocación y documentos justificativos 79
4.8.3 Quién puede solicitar la revocación 81
4.8.4 Procedimiento de solicitud de revocación. 81
4.8.5 Periodo de revocación 82
4.8.6 Suspensión 82
4.8.7 Límites del periodo de suspensión 83
4.8.8 Frecuencia de emisión de CRLs 83
4.8.9 Requisitos de comprobación de CRLs 84
4.8.10 Disponibilidad de comprobación on-line de la revocación 84
4.8.11 Requisitos de la comprobación on-line de la revocación 84
4.8.12 Otras formas de divulgación de información de revocación disponibles 85
4.8.13 Requisitos de comprobación para otras formas de divulgación de información de revocación 85
4.8.14 Requisitos especiales de revocación por compromiso de las claves 85

4.9. Procedimientos de Control de Seguridad 85

4.9.1 Tipos de eventos registrados 85
4.9.2 Periodos de retención para los registros de auditoria 87
4.9.3 Protección de los registros de auditoría 87
4.9.4 Procedimientos de copia de respaldo de los registros de auditoría 87
4.9.5 Sistema de recogida de información de auditoria 87
4.9.6 Notificación al sujeto causa del evento 88
4.9.7 Análisis de vulnerabilidades 88

4.10. Archivo de registros 88

4.10.1 Tipo de archivos registrados. 88
4.10.2 Periodo de retención para el archivo 89
4.10.3 Protección del archivo 89
4.10.4 Procedimientos de copia de respaldo del archivo 89
4.10.5 Requerimientos para el sellado de tiempo de los registros 89
4.10.6 Sistema de recogida de información de auditoria 90
4.10.7 Procedimientos para obtener y verificar información archivada 90

4.11. Cambio de clave 90

4.12. Recuperación en caso de compromiso de la clave o desastre 90

4.12.1 La clave de una entidad se compromete 91
4.12.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre 91

4.13. Cese de la AC 92

5. Controles de Seguridad Física, Procedimental y de Personal 93

5.1.1 Ubicación y construcción 93
5.1.2 Acceso físico 94
5.1.3 Alimentación eléctrica y aire acondicionado 94
5.1.4 Exposición al agua 94
5.1.5 Protección y prevención de incendios 94
5.1.6 Sistema de almacenamiento. 95

5.1.7 Eliminación de residuos 95
5.1.8 Copia de respaldo externa 95

5.2. Controles procedimentales 95
5.2.1 Roles de confianza 95
5.2.2 Número de personas requeridas por tarea 97
5.2.3 Identificación y autentificación para cada rol 97
5.2.4 Arranque y parada del sistema de gestión PKI. 97

5.3. Controles de seguridad de personal 98
5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación 98
5.3.2 Procedimientos de comprobación de antecedentes 99
5.3.3 Requerimientos de formación 99
5.3.4 Requerimientos y frecuencia de la actualización de la formación 100
5.3.5 Frecuencia y secuencia de rotación de tareas 100
5.3.6 Sanciones por acciones no autorizadas 100
5.3.7 Requerimientos de contratación de personal 100
5.3.8 Documentación proporcionada al personal 101

6. Controles de Seguridad Técnica 102

6.1. Generación e instalación del par de claves 102
6.1.1 Generación del par de claves 102
6.1.1.1 Generación del par de claves del Firmante 103
6.1.2 Entrega de la clave pública al emisor del certificado 103
6.1.3 Entrega de la clave pública de la AC a los usuarios 103
6.1.4 Tamaño y periodo de validez de las claves del emisor 103
6.1.5 Tamaño y periodo de validez de las claves del Firmante 104
6.1.1 Parámetros de generación de la clave pública. 104
6.1.2 Comprobación de la calidad de los parámetros 104
6.1.3 Hardware/software de generación de claves 104
6.1.4 Fines del uso de la clave 104

6.2. Protección de la clave privada 107

6.3. Estándares para los módulos criptográficos 108
6.3.1 Control multi-personal (n de entre m) de la clave privada 108
6.3.2 Custodia de la clave privada 109
6.3.3 Copia de seguridad de la clave privada 109
6.3.4 Archivo de la clave privada 109
6.3.5 Introducción de la clave privada en el módulo criptográfico. 110
6.3.6 Método de activación de la clave privada. 110
6.3.7 Método de desactivación de la clave privada 111
6.3.8 Método de destrucción de la clave privada 111

6.4. Otros aspectos de la gestión del par de claves 111
6.4.1 Archivo de la clave pública 111
6.4.2 Periodo de uso para las claves públicas y privadas 112

6.5. Datos de activación de las claves privadas. 112
6.5.1 Generación. 112
6.5.2 Protección de los datos de activación 112
6.5.3 Otros aspectos de los datos de activación 112

6.6. Ciclo de vida del dispositivo cualificado de creación de firma. 112

6.7. Controles de seguridad informática 113
6.7.1 Requerimientos técnicos de seguridad informática específicos 113
6.7.2 Requerimientos técnicos de seguridad informática específicos 114
6.7.3 Valoración de la seguridad informática 114

6.8. Controles de seguridad del ciclo de vida 115
6.8.1 Controles de desarrollo del sistema 115
6.8.2 Controles de gestión de la seguridad 115
6.8.2.1 Gestión de seguridad 115
6.8.2.2 Clasificación y gestión de información y bienes 115
6.8.2.3 Operaciones de gestión 116
6.8.2.4 Gestión del sistema de acceso 117
6.8.2.5 Gestión del ciclo de vida del hardware criptográfico 118
6.8.3 Evaluación de la seguridad del ciclo de vida 119

6.9. Controles de seguridad de la red 119

6.10. Fuentes de Tiempo 119

6.11. Controles de ingeniería de los módulos criptográficos 119

7. Perfiles de Certificado y CRL 120

7.1. Perfil de Certificado 120
7.1.1 Número de versión 120
7.1.2 Extensiones del certificado 120
7.1.3 Identificadores de objeto (OID) de los algoritmos 120
7.1.4 Formato de Nombres. 120
7.1.5 Restricciones de los nombres 121
7.1.6 Identificador de objeto (OID) de la Política de Certificación 121
7.1.1 Uso de la extensión "*Policy Constraints*" 121
7.1.2 Sintaxis y semántica de los calificadores de política 121
7.1.3 Tratamiento semántico para la extensión crítica "*Certificate Policy*" 121

7.2. Perfil de CRL 121
7.2.1 Número de versión 122
7.2.2 CRL y extensiones 122

7.3. Perfil de OCSP 122
7.3.1 Número de versión 122
7.3.2 Extensiones OCSP 122

8. Especificación de la administración. 123

8.1. Autoridad de las políticas 123

8.2. Procedimientos de especificación de cambios. 123
8.2.1 Elementos que pueden cambiar sin necesidad de notificación 123
8.2.2 Cambios con notificación 123
8.2.2.1 Lista de elementos 123
8.2.2.2 Mecanismo de notificación 123
8.2.2.3 Periodo de comentarios 124
8.2.2.4 Mecanismo de tratamiento de los comentarios 124

8.3. Publicación y copia de la política 124

8.4. Procedimientos de aprobación de la CPS 124

9. Anexo I. Acrónimos _____ *125*
10. Anexo II. Definiciones _____ *127*

1. Introducción

1.1. Consideración Inicial

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

Política de Certificación (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 Sujeto/Firmante, la Parte Usuaria y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

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

Una 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.

1.2. Vista General

El Reglamento (UE) 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 (de ahora en adelante, eIDAS), fija como servicios de confianza, los siguientes servicios electrónicos prestados habitualmente a cambio de una remuneración y que consistan en: - la creación, verificación y validación de firmas electrónicas. Se incluyen los certificados relativos a estos

servicios; - la creación, verificación y validación de sellos electrónicos. Se incluyen los certificados relativos a estos servicios; - la creación, verificación y validación de sellos de tiempo electrónicos. Se incluyen los certificados relativos a estos servicios; la entrega electrónica certificada. Se incluyen los certificados relativos a estos servicios; - la creación, verificación y validación de certificados para la autenticación de sitios web, y - la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

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 servicios de confianza basados en los siguientes estándares:

Servicio	EN general	EN de alcance	Perfiles/semántica
Creación, verificación y validación de firmas electrónicas.	EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers	319 411-1 v1.1.1: General requirements 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates	EN 319 412 Certificate Profiles - 319 412-1 v1.1.1: Overview and common data structures - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons - 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations - 319 412-5 v2.1.1: QCStatements
La creación, verificación y validación de sellos electrónicos. Se incluyen los certificados relativos a estos servicios;	EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers	319 411-1 v1.1.1: General requirements 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates	319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons
La creación, verificación y validación de sellos de tiempo electrónicos. Se incluyen los certificados relativos a estos servicios;	EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers	EN 319 421 v1.1.1: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps	EN 319 422 v1.1.1 Time-stamping protocol and electronic time-stamp profiles
Creación, verificación y validación de certificados para la autenticación de sitios web, y	EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers	319 411-1 v1.1.1: General requirements 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates	319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations

Respecto a las políticas a aplicar según EN 319 411-1 / 2 se describen los siguientes grupos de políticas:

Políticas generales:

- **NCP** Política de certificación normalizada.
- **NCP+** Política de certificación normalizada con dispositivo seguro.
- **LCP** Política de certificación ligera (sin presencia física).
- **EVCP** Política de certificación de certificados validación extendida.
- **DVCP** Política de certificación de certificados validación de dominio.
- **OVCP** Política de certificación de certificados validación de organización.

Políticas para certificados cualificados:

- **QCP-n** Políticas para certificados cualificados emitidos a personas físicas. Incorpora los requisitos de la política **NCP** más requerimientos adicionales para dar soporte a la gestión de certificados cualificados.
- **QCP-l** Políticas para certificados cualificados emitidos a personas jurídicas. Incorpora los requisitos de la política **NCP** más requerimientos adicionales para dar soporte a la gestión de certificados cualificados.
- **QCP-n-qscd** Políticas para certificados cualificados emitidos a personas físicas con DSCF. Incorpora los requisitos de la política **QCP-n** (**NCP+** incluido) más requerimientos adicionales para dar soporte a la gestión de certificados cualificados y la provisión de dispositivos seguros de creación de firma.
- **QCP-l-qscd** Políticas para certificados cualificados emitidos a personas físicas con DSCF. Incorpora los requisitos de la política **QCP-l** (**NCP+** incluido) más requerimientos adicionales para dar soporte a la gestión de certificados cualificados y la provisión de dispositivos seguros de creación de firma.
- **QCP-w** Políticas para certificados cualificados emitidos a servidores web. Cuando el certificado se emite a una persona jurídica incorpora los requisitos de la política **OVCP** o **EVCP** más requerimientos adicionales para dar soporte a la gestión de certificados cualificados. Cuando el certificado se emite a persona física incorpora los requisitos de la política **NCP** más requerimientos adicionales para dar soporte a la gestión de certificados cualificados.

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*.

Estas prácticas están alineadas con los requisitos marcados en *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* elaborado por el CA/BROWSER FORUM http://www.cabforum.org en su versión 1.5.4.

Esta CPS se encuentra en conformidad con las Políticas de Certificación de los diferentes certificados emitidos por Camerfirma que vienen descritos en el apartado **1.2.1** de esta CPS. En caso de contradicción entre los dos documentos prevalecerá lo dispuesto en este documento.

1.2.1 Jerarquías

En este apartado presentaremos las jerarquías y Autoridades de Certificación (en adelante CA, CAs, 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. El OID de los certificados emitidos por cada Autoridad de Certificación para la emisión de certificados de respondedor OCSP es **1.3.6.1.4.1.17326.10.9.8**

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 cambie en su denominación incorporando el año de creación del certificado al final de dicho nombre, no obstante, sus características seguirán siendo las mismas, a no ser que así se indique en esta CPS.

Esta CPS se aplica a partir de las jerarquías **Chambers of Commerce Root 2016** y **Global Chambersign Root 2016**.

1.2.1.1 Emisión de certificados del set de pruebas y certificados de pruebas en general.

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 la Parte Usuaria 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

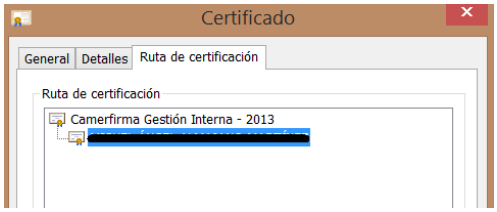
En casos donde el proceso de homologación y evaluación se necesite la emisión de un certificado de pruebas con datos reales, el proceso se realiza después de la firma de un acuerdo de confidencialidad con el organismo encargado de hacer las tareas de homologación o evaluación. Los datos serán los específicos 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.

Para los certificados de servidor no se generan certificados de pruebas.

1.2.1.2 Jerarquía Camerfirma Gestión Interna.

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

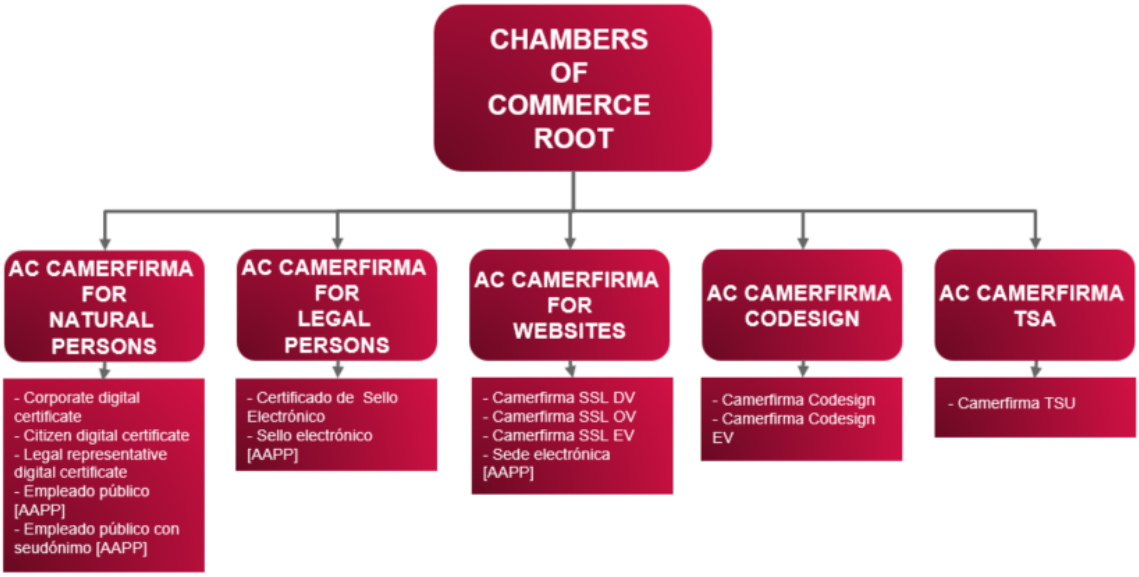
Esta jerarquía está compuesta por una única AC que emite certificado de entidad final.



Como diseño general en el nombre del titula 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

1.2.1.3 Jerarquía CHAMBERS OF COMMERCE.

Esta jerarquía se aplica a partir de CHAMBERS OF COMMERCE - 2016. "CHAMBERS OF COMMERCE ROOT" ES PROPIEDAD DE **AC CAMERFIRMA SA** TAL COMO SE INDICA EN EL CAMPO ORGANIZACIÓN DEL ATRIBUTO CN DEL CERTIFICADO RAIZ CORRESPONDIENTE.



CHAMBERS OF COMMERCE - Any Policy

Huella Digital SHA256
04:F1:BE:C3:69:51:BC:14:54:A9:04:CE:32:89:0C:5D:A3:CD:E1:35:6B:79:00:F6:E6:2D:FA:20:41:EB:AD:51
Huella Digital SHA-1
2D:E1:6A:56:77:BA:CA:39:E1:D6:8C:30:DC:B1:4A:BE:22:A6:17:9B

Esta jerarquía está diseñada para desarrollar una red de confianza con el objeto fundamental de emitir certificados digitales de identidad empresarial, colegial y administración pública, dentro del territorio de la unión europea y donde las Autoridades de Registro (en adelante RA o RAs) son gestionadas por las Cámaras de Comercio, Industria y Navegación de España o entidades públicas o privadas.

EXCEPCIONES: Los certificados de componente (AC CAMERFIRMA CODESIGN, AC CAMERFIRMA TSA Y AC CAMERFIRMA FOR WEBSITES) no tienen limitación territorial ni están asociadas a entidades de registro concretas.

Bajo esta CPS se permite la emisión de certificados de Autoridad de Certificación intermedias correspondientes a un colectivo empresarial, colegial o público concreto, siempre que el ámbito de aplicación sea el territorio de la unión europea. De esta forma los certificados emitidos bajo esta autoridad de certificación intermedia adquieren los reconocimientos obtenidos por la ROOT en los aplicativos comerciales (léase: Navegadores como Internet Explorer, Google Chrome, Mozilla Firefox, etc.).

Por otro lado, el esquema de Autoridades de Certificación intermedias que emiten certificados digitales bajo esta jerarquía son:

AC CAMERFIRMA FOR NATURAL PERSONS 2016	
1.3.6.1.4.1.17326.10.16.1.1	**CITIZEN DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.10.16.1.1.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Ciudadano en QSCD
1.3.6.1.4.1.17326.10.16.1.1.2 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Ciudadano
1.3.6.1.4.1.17326.10.16.1.2	**CORPORATE DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.10.16.1.2.1 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** Corporativo en QSCD
1.3.6.1.4.1.17326.10.16.1.2.2 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** Corporativo
1.3.6.1.4.1.17326.10.16.1.3	**LEGAL REPRESENTATIVE DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.10.16.1.3.1.1 2.16.724.1.3.5.8 [normativa nacional] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Representante de Persona Jurídica con Poderes Generales de Representación en QSCD
1.3.6.1.4.1.17326.10.16.1.3.1.2 2.16.724.1.3.5.8 [normativa nacional] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Representante de Persona Jurídica con Poderes Generales de Representación
1.3.6.1.4.1.17326.10.16.1.3.1.1 2.16.724.1.3.5.9 [normativa nacional] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Representante de Entidad Sin Personalidad Jurídica con Poderes Generales de Representación en QSCD
1.3.6.1.4.1.17326.10.16.1.3.1.2 2.16.724.1.3.5.9 [normativa nacional] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Representante de Entidad Sin Personalidad Jurídica con Poderes Generales de Representación
1.3.6.1.4.1.17326.10.16.1.3.2.1 2.16.724.1.3.5.8 [normativa nacional] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Representante de Persona Jurídica para trámites con las AAPP en QSCD
1.3.6.1.4.1.17326.10.16.1.3.2.2 2.16.724.1.3.5.8 [normativa nacional] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Representante de Persona Jurídica para trámites con las AAPP
1.3.6.1.4.1.17326.10.16.1.3.2.1 2.16.724.1.3.5.9 [normativa nacional] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Representante de Entidad Sin Personalidad Jurídica para trámites con las AAPP en QSCD
1.3.6.1.4.1.17326.10.16.1.3.2.2 2.16.724.1.3.5.9 [normativa nacional] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Representante de Entidad Sin Personalidad Jurídica para trámites con las AAPP
1.3.6.1.4.1.17326.10.16.1.3.3.1 2.16.724.1.3.5.8 [normativa nacional] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Representante de Persona Jurídica para Apoderados en QSCD
1.3.6.1.4.1.17326.10.16.1.3.3.2 2.16.724.1.3.5.8 [normativa nacional] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Representante de Persona Jurídica para Apoderados

1.3.6.1.4.1.17326.10.16.1.3.3.1 2.16.724.1.3.5.9 [normativa nacional] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Representante de Entidad Sin Personalidad Jurídica para Apoderados en QSCD
1.3.6.1.4.1.17326.10.16.1.3.3.2 2.16.724.1.3.5.9 [normativa nacional] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Representante de Entidad Sin Personalidad Jurídica para Apoderados
1.3.6.1.4.1.17326.10.16.1.5	**EMPLEADO PÚBLICO [AAPP]**
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 2.16.724.1.3.5.7.1 [AAPP empleado público nivel alto] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Empleado Público de Firma en QSCD. Nivel Alto.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 2.16.724.1.3.5.7.1 [AAPP empleado público nivel alto] 0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+]	Certificado de Empleado Público de Autenticación en QSCD. Nivel Alto.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 2.16.724.1.3.5.7.1 [AAPP empleado público nivel alto]	Certificado de Empleado Público de Cifrado. Nivel Alto.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.7.2 [AAPP empleado público nivel medio] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Empleado Público en QSCD. Nivel Medio.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.7.2 [AAPP empleado público nivel medio] 0.4.0.194112.1.0 [ETSI EN 319 411 2 – QCP-n]	Certificado **Cualificado** de Empleado Público. Nivel Medio.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1 2.16.724.1.3.5.4.1 [AAPP empleado público nivel alto] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Empleado Público con Seudónimo de Firma en QSCD. Nivel Alto.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2 2.16.724.1.3.5.4.1 [AAPP empleado público nivel alto] 0.4.0.2042.1.2 [ETSI EN 319 411 1 - NCP+]	Certificado de Empleado Público con Seudónimo de Autenticación en QSCD. Nivel Alto.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3 2.16.724.1.3.5.4.1 [AAPP empleado público nivel alto]	Certificado de Empleado Público con Seudónimo de Cifrado. Nivel Alto.
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.4.2 [AAPP empleado público nivel medio] 0.4.0.194112.1.2 [ETSI EN 319 411 2 - QCP-n-qscd]	Certificado **Cualificado** de Empleado Público con Seudónimo en QSCD
1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4 2.16.724.1.3.5.4.2 [AAPP empleado público nivel medio] 0.4.0.194112.1.0 [ETSI EN 319 411 2 - QCP-n]	Certificado **Cualificado** de Empleado Público con Seudónimo. Nivel Medio.
AC CAMERFIRMA FOR LEGAL PERSONS 2016	
1.3.6.1.4.1.17326.10.16.2.1	**ELECTRONIC SEAL QUALIFIED DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.10.16.2.1.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]	Certificado **Cualificado** de Sello Electrónico en QSCD
1.3.6.1.4.1.17326.10.16.2.1.2 0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l]	Certificado **Cualificado** de Sello Electrónico
1.3.6.1.4.1.17326.10.16.2.3	**ELECTRONIC SEAL DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.10.16.2.3.2 0.4.0.2042.1.3 [ETSI EN 319 411 1 - LCP]	Certificado de Sello Electrónico
1.3.6.1.4.1.17326.10.16.2.2	**SELLO ELECTRÓNICO (AAPP)**

1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] 2.16.724.1.3.5.6.1 [AAPP - sello nivel alto]	Certificado **Cualificado** de Sello Electrónico AAPP en QSCD. Nivel Alto.
1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] OID 2.16.724.1.3.5.6.2 [AAPP sello nivel medio]	Certificado **Cualificado** de Sello Electrónico AAPP en QSCD. Nivel Medio.
1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l] OID 2.16.724.1.3.5.6.2 [AAPP sello nivel medio]	Certificado **Cualificado** de Sello Electrónico AAPP. Nivel Medio.
AC CAMERFIRMA FOR WEBSITES	
1.3.6.1.4.1.17326.10.16.3.2	**CAMERFIRMA SSL OV**
1.3.6.1.4.1.17326.10.16.3.2.2 0.4.0.2042.1.7 [ETSI TS 102 042 - OVCP] 2.23.140.1.2.2 [CA/B FORUM - SSL OV]	Certificado de Website OV
1.3.6.1.4.1.17326.10.16.3.5	**CAMERFIRMA SSL EV**
1.3.6.1.4.1.17326.10.16.3.5.1 0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w] 2.23.140.1.1 [CA/B FORUM - SSL EV]	Certificado **Cualificado** de Website EV
1.3.6.1.4.1.17326.10.16.3.6	**SEDE ELECTRÓNICA ADMINISTRATIVA (AAPP)**
1.3.6.1.4.1.17326.10.16.3.6.1.3.2.1 0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w] 2.16.724.1.3.5.5.1 [AAPP - sede nivel alto] 2.23.140.1.1 [CA/B FORUM - SSL EV]	Certificado **Cualificado** de Sede Electrónica - Nivel Alto - EV
1.3.6.1.4.1.17326.10.16.3.6.1.3.2.2 0.4.0.194112.1.4 [ETSI EN 319 411 2 - QCP-w] 2.16.724.1.3.5.5.2 [AAPP - sede nivel medio] 2.23.140.1.1 [CA/B FORUM - SSL EV]	Certificado **Cualificado** de Sede Electrónica - Nivel Medio – EV
AC CAMERFIRMA CODESIGN	
1.3.6.1.4.1.17326.10.16.4.1	**CAMERFIRMA CODESIGN**
1.3.6.1.4.1.17326.10.16.4.1.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]	Certificado **Cualificado** de Firma de Código en QSCD
1.3.6.1.4.1.17326.10.16.4.1.2 0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l]	Certificado **Cualificado** de Firma de Código
1.3.6.1.4.1.17326.10.16.4.2	**CAMERFIRMA EV CODESIGN**
1.3.6.1.4.1.17326.10.16.4.2.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd] 2.23.140.1.3 [CA/B FORUM - CODESIGN]	Certificado **Cualificado** de Firma de Código EV en QSCD
1.3.6.1.4.1.17326.10.16.4.2.2 0.4.0.194112.1.1 [ETSI EN 319 411 2 - QCP-l] 2.23.140.1.3 [CA/B FORUM - CODESIGN]	Certificado **Cualificado** de Firma de Código EV
AC CAMERFIRMA TSA	
1.3.6.1.4.1.17326.10.16.5.1	**CAMERFIRMA TSU**
1.3.6.1.4.1.17326.10.16.5.1.1 0.4.0.194112.1.3 [ETSI EN 319 411 2 - QCP-l-qscd]	Certificado **Cualificado** de TSU en QSCD
1.3.6.1.4.1.17326.10.16.5.1.2	Certificado de TSU

1.2.1.3.1 AC CAMERFIRMA FOR WEBSITES. (Certificados para sitios web)

Es una AC intermedia que emite certificados digitales a aplicativos servidores de páginas HTML en Internet mediante protocolo TLS. Este protocolo es necesario para la identificación y el establecimiento de canales seguros entre el navegador de la Parte Usuaria y el servidor de páginas HTML del Sujeto/Firmante.

Bajo esta CPS se permite la emisión de certificados a entidades u organismos que residan fuera de territorio de la unión europea. El procedimiento de emisión del certificado se tratará en el apartado correspondiente de esta CPS.

Se emiten certificados en diferentes modalidades:

1.2.1.3.1.1 Certificados de Website OV (*Organization Validation*) – OVCP.

La emisión de este tipo de certificados cumple los requisitos establecidos por el documento *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* elaborado por el CA/BROWSER FORUM http://www.cabforum.org. Los procesos de registro llevados a cabo incorporan la validación de una organización asociada al control de dominio.

1.2.1.3.1.2 Certificados Cualificados de Website EV (*Extended Validation*) – EVCP. La emisión de certificados digitales para Servidor Seguro EV cumple los requisitos establecidos por el documento Guidelines for Issuance and Management of extended validation certificates elaborado por el CA/BROWSER FORUM http://www.cabforum.org. Esta normativa impulsa la emisión de certificados de servidor seguro con garantías adicionales en el proceso de identificación de los titulares de los certificados.
Un certificado de Website certificado EV permite a los navegadores que se conectan a este servicio, un nivel de aseguramiento adicional; este hecho lo visualizan mostrando un fondo verde en la línea de direcciones del navegador.

1.2.1.3.1.3 Certificados Cualificados de Sede electrónica OV y EV - QCP-w.

Establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

1.2.1.3.2 AC CAMERFIRMA FOR LEGAL PERSONS. (Certificados para personas jurídicas).

1.2.1.3.2.1 Certificado Cualificado de Sello Electrónico – QCP-l, QCP-l-qscd.

Este certificado se emite a una persona jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y

transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

1.2.1.3.2.2 Certificado de Sello Electrónico – LCP.

Este certificado se emite a una persona jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

1.2.1.3.2.3 Certificado de Sello Electrónico AAPP. QCP-l, QCP-l-qscd

Establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

1.2.1.3.3 AC CAMERFIRMA CODESIGN. (Certificados para firma de código).

AC intermedio llamada "AC CAMERFIRMA CODESIGN" que emite certificados para la firma de código. Los certificados de 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.

Bajo esta CPS se permite la emisión de certificados a entidades u organismos que residan fuera de territorio español. El procedimiento de emisión del certificado se tratará en el apartado correspondiente de esta CPS.

Se emiten certificados en diferentes modalidades:

1.2.1.3.3.1 Certificados Cualificados de Firma de Código – QCP-l, QCP-l-qscd.

La emisión de este tipo de certificados cumple los requisitos establecidos por el documento *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* elaborado por el CA/BROWSER FORUM http://www.cabforum.org. Los procesos de registro llevados a cabo incorporan la validación de una organización asociada al control de dominio.

1.2.1.3.3.2 Certificados Cualificados de Firma de Código EV (*Extended Validation*) – QCP-l, QCP-l-qscd.

La emisión de certificados digitales de firma de código EV está sujeta a los requerimientos establecidos por el documento *Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates* elaborado por el CA/BROWSER FORUM http://www.cabforum.org. Esta normativa impulsa la emisión de certificados de firma de código con garantías adicionales en el proceso de identificación de los titulares de los certificados.

1.2.1.3.4 AC CAMERFIRMA TSA. (Certificados para Sellado de tiempo)

Esta autoridad 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 emitidos por Camerfirma por defecto 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 CPS 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 CPS.

AC Camerfirma emite certificados de TSU en **equipos homologados** por AC Camerfirma. Los equipos homologados pueden estar localizados en las instalaciones del cliente. El cliente debe firmar una declaración responsable en el que se compromete al cumplimiento de los requisitos asociados a las políticas y prácticas de certificación de AC Camerfirma SA.

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 140-2 Nivel 3) 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:

1.2.1.3.4.1 Certificado Cualificado de TSU en QSCD

Las claves se generan y almacenan en un HSM FIPS 140-2 certificado nivel 3.

1.2.1.3.4.2 Certificado de TSU

Las claves se generan y almacenan en soporte software.

El acceso al servicio puede ser autenticado por usuario/contraseña o por certificado digital vía protocolo HTTPS. Se permite también las implantaciones de autenticación por IP.

Más información en http://www.camerfirma.com/servicios/sellado-de-tiempo

1.2.1.3.5 AC CAMERFIRMA FOR NATURAL PERSONS. (Certificados para personas físicas)

Estamos ante una Autoridad de Certificación multi-política, que emite certificados cualificados y no cualificados de a persona físicas dentro del territorio de la unión europea cuyas funcionalidades se describen a continuación.

Los certificados finales se dirigen a:

1.2.1.3.5.1 Personas físicas con atributo de vinculación a Entidad.

1.2.1.3.5.1.1 Certificado Cualificado Corporativo – QCP-n, QCP-n-qscd.

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

1.2.1.3.5.1.2 Certificado Cualificado de Representante Legal:

1.2.1.3.5.1.2.1 Certificado Cualificado de Representante de Persona Jurídica con Poderes Generales de Representación. – QCP-n, QCP-n-qscd.

Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/Sujeto/Firmante) y una entidad con personalidad jurídica (descrita también en el campo Organización del certificado).

1.2.1.3.5.1.2.2 Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica con Poderes Generales de Representación. – QCP-n, QCP-n-qscd.

Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/Sujeto/Firmante) y una entidad sin personalidad jurídica (descrita también en el campo Organización del certificado).

1.2.1.3.5.1.2.3 Certificado Cualificado de Representante Persona Jurídica para trámites con las AAPP. – QCP-n, QCP-n-qscd.

Tiene por objeto identificar a una persona física y añade el atributo (información) de que dicha persona puede representar a una entidad con personalidad jurídica en el ámbito de la Administración Pública.

1.2.1.3.5.1.2.4 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica para trámites con las AAPP. – QCP-n, QCP-n-qscd.

Tiene por objeto identificar a una persona física y añade el atributo (información) de que dicha persona puede representar a una entidad sin personalidad jurídica en el ámbito de la Administración Pública.

1.2.1.3.5.1.2.5 Certificado Cualificado de Representante de Persona Jurídica para Apoderados. – QCP-n, QCP-n-qscd.

Determina la relación de representación específica o de apoderamiento especial entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad con personalidad jurídica (descrita también en el campo Organización del certificado).

1.2.1.3.5.1.2.6 Certificado Cualificado de Representante de Entidad sin Personalidad Jurídica para Apoderados. – QCP-n, QCP-n-qscd.

Determina la relación de representación específica o de apoderamiento especial entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad sin personalidad jurídica (descrita también en el campo Organización del certificado).

1.2.1.3.5.1.3 Certificados de Empleado Público. – QCP-n, QCP-n-qscd, NCP+.

Establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Dentro del marco jurídico establecen 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.

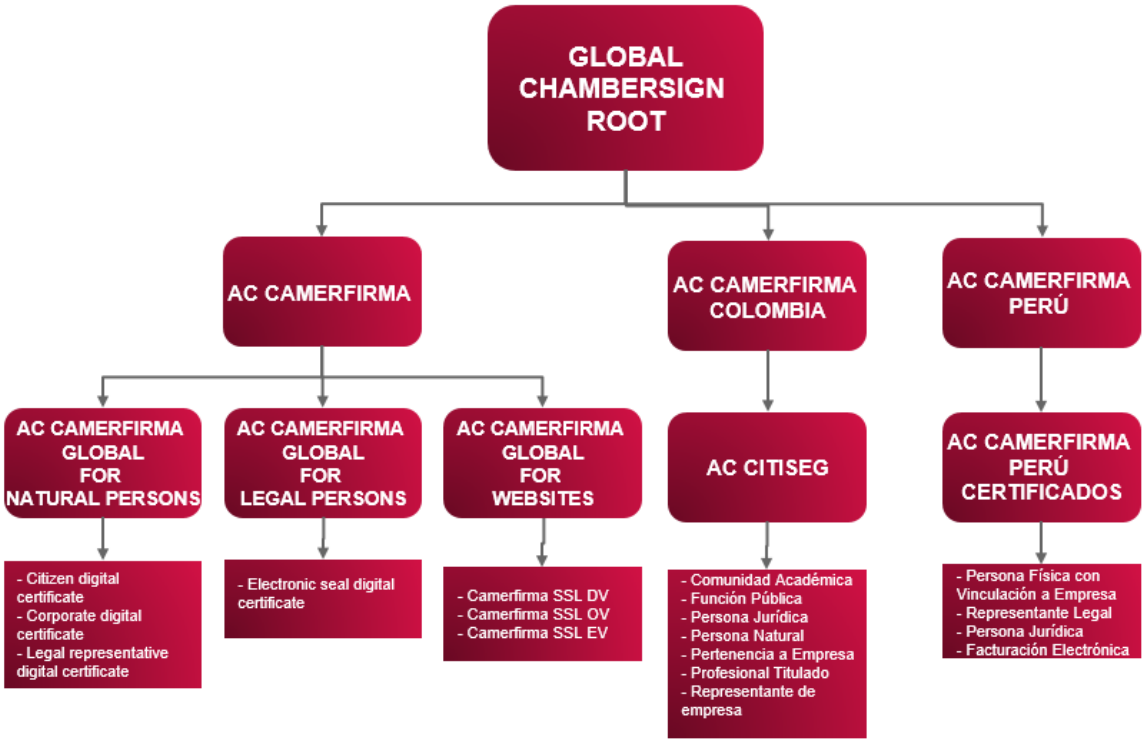
1.2.1.3.5.2 Personas físicas SIN atributo de vinculación a Entidad.

1.2.1.3.5.2.1 Certificado Cualificado de Ciudadano. – QCP-n, QCP-n-qscd.

Determina la identidad de la persona física firmante para actuar en su propio nombre.

1.2.1.4 Jerarquía GLOBAL CHAMBERSIGN ROOT.

Esta jerarquía se aplica a partir de GLOBAL CHAMBERSIGN ROOT - 2016. "GLOBAL CHAMBERSIGN ROOT" ES PROPIEDAD DE **AC CAMERFIRMA SA** TAL COMO SE INDICA EN EL CAMPO ORGANIZACIÓN DEL ATRIBUTO CN CERTIFICADO RAIZ CORRESPONDIENTE.



GLOBAL CHAMBERSIGN ROOT - AnyPolicy.

Huella Digital SHA-256
C1:D8:0C:E4:74:A5:11:28:B7:7E:79:4A:98:AA:2D:62:A0:22:5D:A3:F4:19:E5:C7:ED:73:DF:BF:66:0E:71:09
Huella Digital SHA-1
11:39:A4:9E:84:84:AA:F2:D9:0D:98:5E:C4:74:1A:65:DD:5D:94:E2

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. Esta Jerarquía por lo tanto puede emitir certificados en cualquier parte donde exista una RA reconocida que cumpla los requisitos establecidos por Camerfirma y **sujetándose en todo caso a la legislación vigente aplicable a las relaciones comerciales internacionales**.

La jerarquía Chambersign Global Root organiza la emisión de certificados digitales en diferentes territorios 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 correspondiente.

En el marco de esta jerarquía se desarrollan distintas Autoridades de Certificación intermedias que corresponderán a marcos globales, nacionales, sectoriales o empresariales.

GLOBAL CHAMBERSIGN ROOT - 2016	
AC CAMERFIRMA	
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS	
1.3.6.1.4.1.17326.20.16.1.1.1	**CITIZEN DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.20.16.1.1.1.1	Certificado de Ciudadano en QSCD
1.3.6.1.4.1.17326.20.16.1.1.1.2	Certificado de Ciudadano
1.3.6.1.4.1.17326.20.16.1.1.2	**CORPORATE DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.20.16.1.1.2.1	Certificado Corporativo en QSCD
1.3.6.1.4.1.17326.20.16.1.1.2.2	Certificado Corporativo
1.3.6.1.4.1.17326.20.16.1.1.3	**LEGAL REPRESENTATIVE DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.20.16.1.1.3.1.1	Certificado de Representante de Persona Jurídica en QSCD
1.3.6.1.4.1.17326.20.16.1.1.3.1.2	Certificado de Representante de Persona Jurídica
1.3.6.1.4.1.17326.20.16.1.1.3.2.1	Certificado de Representante de Entidad Sin Personalidad Jurídica en QSCD
1.3.6.1.4.1.17326.20.16.1.1.3.2.2	Certificado de Representante de Entidad Sin Personalidad Jurídica
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS	
1.3.6.1.4.1.17326.20.16.1.2.1	**ELECTRONIC SEAL DIGITAL CERTIFICATE**
1.3.6.1.4.1.17326.20.16.1.2.1.1.1	Certificado de Sello Electrónico en QSCD
1.3.6.1.4.1.17326.20.16.1.2.1.1.2	Certificado de Sello Electrónico
AC CAMERFIRMA GLOBAL FOR WESITES	
1.3.6.1.4.1.17326.10.8.12	**CAMERFIRMA SSL EV**
1.3.6.1.4.1.17326.10.8.12.1.2	Certificado de Website EV
AC CAMERFIRMA COLOMBIA	
AC CITISEG	
1.3.6.1.4.1.17326.20.1.1	**COMUNIDAD ACADÉMICA**
1.3.6.1.4.1.17326.20.1.1.2	Certificado de Comunidad Académica
1.3.6.1.4.1.17326.20.1.2	**FUNCIÓN PÚBLICA**
1.3.6.1.4.1.17326.20.1.2.2	Certificado de Función Pública
1.3.6.1.4.1.17326.20.1.3	**PERSONA JURÍDICA**
1.3.6.1.4.1.17326.20.1.3.2	Certificado de Persona Jurídica
1.3.6.1.4.1.17326.20.1.4	**PERSONA NATURAL**
1.3.6.1.4.1.17326.20.1.4.2	Certificado de Persona Natural
1.3.6.1.4.1.17326.20.1.5	**PERTENENCIA A EMPRESA**
1.3.6.1.4.1.17326.20.1.5.2	Certificado de Pertenencia a Empresa
1.3.6.1.4.1.17326.20.1.6	**PROFESIONAL TITULADO**
1.3.6.1.4.1.17326.20.1.6.2	Certificado de Profesional Titulado

1.3.6.1.4.1.17326.20.1.7	**REPRESENTANTE DE EMPRESA**
1.3.6.1.4.1.17326.20.1.7.2	Certificado de Representante de Empresa
AC CAMERFIRMA PERÚ **AC CAMERFIRMA PERÚ CERTIFICADOS**	
1.3.6.1.4.1.17326.30.16.0	**PERSONA FÍSICA CON VINCULACIÓN A EMPRESA**
1.3.6.1.4.1.17326.30.16.0.1	Certificado de Persona Física con Vinculación a Empresa
1.3.6.1.4.1.17326.30.16.10	**REPRESENTANTE LEGAL**
1.3.6.1.4.1.17326.30.16.10.1	Certificado de Representante Legal
1.3.6.1.4.1.17326.30.16.20	**PERSONA JURÍDICA**
1.3.6.1.4.1.17326.30.16.20.1	Certificado de Persona Jurídica
1.3.6.1.4.1.17326.30.16.30	**FACTURACIÓN ELECTRÓNICA**
1.3.6.1.4.1.17326.30.16.30.1	Certificado de Facturación Electrónica

1.2.1.4.1 AC CAMERFIRMA.

El objeto de esta AC intermedia será la de emitir certificados de AC subordinada sin restricciones en ámbito geográfico, sectorial o autoridad de registro concreta.

1.2.1.4.1.1 AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS (Certificados para personas físicas)

Esta Autoridad de certificación emite certificados para personas físicas sin restricciones en ámbito geográfico, sectorial o autoridad de registro concreta.

1.2.1.4.1.1.1 Personas físicas CON atributo de vinculación a Entidad.

1.2.1.4.1.1.1.1 Certificado Corporativo.

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

1.2.1.4.1.1.1.2 Certificado de Representante de Persona Jurídica.

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

1.2.1.4.1.1.1.3 Certificado de Representante de Entidad sin Personalidad Jurídica.

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

1.2.1.4.1.1.2 Personas físicas SIN atributo de vinculación a Entidad.

1.2.1.4.1.1.2.1 Certificado de Ciudadano.

Determina la identidad de la persona física firmante para actuar en su propio nombre.

1.2.1.4.1.2 AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS. (Certificados para personas jurídicas)

1.2.1.4.1.2.1 Certificado de Sello Electrónico.

Este certificado se emite a una entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

1.2.1.4.1.3 AC CAMERFIRMA GLOBAL FOR WEBSITES. (Certificados para sitios web). EVCP.

Es una AC intermedia que emite certificados digitales a aplicativos servidores de páginas HTML en Internet mediante protocolo TLS. Este protocolo es necesario para la identificación y el establecimiento de canales seguros entre el navegador de la Parte Usuaria y el servidor de páginas HTML del Sujeto/Firmante.

Esta AC emite certificados de la misma forma y alcance que su equivalente en la jerarquía Chambers of Commerce Root. La activación de esta AC solo se usará a efectos de realizar los procesos de acreditación con los distintos navegadores. En los procesos de acreditación el prestador tiene que activar una serie de sitios web protegidos con los certificados de SSL emitidos dentro de las jerarquías de certificación que se necesitan reconocer en los distintos almacenes de confianza.

1.2.1.4.2 AC CAMERFIRMA COLOMBIA.

El objeto de esta AC intermedia será la de emitir certificados de AC subordinada dentro del ámbito geográfico de la República de Colombia.

1.2.1.4.2.1 AC CITISEG (Certificados para personas físicas y jurídicas)

1.2.1.4.2.1.1 Certificado de Comunidad Académica (Certificados para personas físicas)

Determinan la relación de vinculación laboral o mercantil entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad Académica (campo organización del certificado).

1.2.1.4.2.1.2 Certificado de Función Pública (Certificados para personas físicas)

Determinan la relación de vinculación laboral entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad perteneciente a la Administración Pública de la Republica de Colombia (campo organización del certificado).

1.2.1.4.2.1.3 Certificado de Persona Jurídica (Certificados para personas jurídicas)

Este certificado se emite a una entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

1.2.1.4.2.1.4 Certificado de Persona Natural (Certificados para personas físicas)

Determina la identidad de la persona física firmante para actuar en su propio nombre.

1.2.1.4.2.1.5 Certificado de Pertenencia a Empresa (Certificados para personas físicas)

Determinan la relación de vinculación laboral o mercantil entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad (campo organización del certificado).

1.2.1.4.2.1.6 Certificado de Profesional Titulado (Certificados para personas físicas)

Determinan la relación de vinculación colegial entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad Colegiada (campo organización del certificado).

1.2.1.4.2.1.7 Certificado de Representante de Empresa (Certificados para personas físicas)

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

1.2.1.4.3 AC CAMERFIRMA PERÚ.

El objeto de esta AC intermedia será la de emitir certificados de AC subordinada dentro del ámbito geográfico de la República del Perú.

Esta autoridad de certificación se desplegó en Agosto de 2017 después de haber recibido la autorización del organismo supervisor nacional INDECOPI.

1.2.1.4.3.1 AC CAMERFIRMA PERÚ CERTIFICADOS (Certificados para personas físicas y jurídicas)

1.2.1.4.3.1.1 Certificado de Persona Física con Vinculación Pertenencia a Empresa (Certificados para personas físicas)

Determinan la relación de vinculación laboral o mercantil entre una persona física (titular del certificado/Sujeto/Firmante) y una Entidad (campo organización del certificado).

1.2.1.4.3.1.2 Certificado de Representante Legal (Certificados para personas físicas)

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

1.2.1.4.3.1.3 Certificado de Persona Jurídica (Certificados para personas jurídicas)

Este certificado se emite a una entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. Este certificado puede estar asociado a una clave activada por una máquina o aplicativo. Las operaciones realizadas comúnmente se realizan de forma automática y desasistida. La acción de las claves se asocia al uso de un certificado de sello electrónico dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se permite

usarse como elemento de identificación cliente de maquina en protocolos de comunicación seguros TLS.

1.2.1.4.3.1.4 Certificado de Factura Electrónica (Certificados para personas físicas)

Este certificado es exclusivo para la realización de facturas electrónicas y se emite a una entidad jurídica cuyo solicitante debe tener representación o autorización de la entidad incluida en el certificado. La acción de las claves se asocia al uso de un certificado de vinculación dota de integridad y autenticidad a las facturas sobre los que se aplica.

1.3. 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.

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.

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

E-mail:	juridico@camerfirma.com las direcciones postales, teléfonos y fax se encuentran publicadas en https://www.camerfirma.com/address

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.

1.4. Identificación

Nombre:	CPS Camerfirma SA.

Descripción:	Documento de respuesta a los requerimientos de las Políticas descritas e identificadas en los puntos previos de este documento donde se describen las jerarquías afectadas.
Versión:	Ver página inicial
OID	1.3.6.1.4.1.17326.10.1
Localización:	https://policy.camerfirma.com/

1.5. Comunidad y Ámbito de Aplicación.

1.5.1 Autoridad de Certificación (AC).

Es el componente de una PKI responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Sujeto (Firmante) y la Parte Usuaria, en las relaciones electrónicas, vinculando una determinada clave pública con una persona. La AC tiene la responsabilidad final en la provisión de los servicios de certificación. La AC está identificada en el campo Asunto (*Issuer*) del certificado digital.

Una AC es un tipo de prestador de servicios de confianza (TSP) que emite certificados digitales.

Un TSP puede incorporar una jerarquía de AC. Esta jerarquía de AC enlaza con una AC raíz. El TSP es responsable que todas las AC incorporadas en la jerarquía cumplan con los requisitos de las políticas correspondientes. Pueden 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.

Una Autoridad de certificación (AC) utiliza Autoridades de registro (RA) para realizar las labores de comprobación y almacenamiento de la documentación de los contenidos incorporados en el certificado digital. En cualquier momento la AC puede cubrir las labores de una RA.

Una AC pertenece a una entidad jurídica indicada en el atributo organización (O) del campo emisor (*Issuer*) 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

1.5.2 Autoridad de Certificación Intermedia o subordinada.

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

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

El certificado de una AC subordinada es firmado por un certificado *root* AC (entidad raíz origen de la jerarquía de certificación) u otra AC subordinada.

Una AC subordinada puede ser objeto de limitaciones por la AC de la cual depende jerárquicamente:

a) Técnicamente mediante una combinación de los siguientes parámetros dentro del certificado: *Extended Key Usage* y *Name Constraints*
b) Contractualmente.

Una Autoridad intermedia puede identificarse como interna o externa. Una **AC subordinada Interna** es propiedad de la misma organización que la AC de la que depende jerárquicamente en este caso AC Camerfirma. Por el contrario, una **AC subordinada 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.

1.5.3 Entidad de Acreditación u Organismo de Supervisión.

La entidad de supervisión será el órgano gestor correspondiente que admite, acredita y supervisa a los TSP dentro de un ámbito geográfico concreto. Esta tarea dentro del Estado Español recae en el Ministerio de Energía, Turismo y Agenda Digital, siendo la autoridad competente dependiendo del Estado Español miembro del Espacio Económico Europeo.

Las AC subordinadas 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.

1.5.4 Prestador de servicios de confianza (TSP).

Un prestador de servicios de confianza (TSP) es una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.

Un prestador de servicios de confianza cualificado presta uno o varios servicios de confianza cualificados y que el organismo de supervisión ha concedido la cualificación

Dentro de los servicios de confianza definidos en eIDAS se encuentran:

- La creación, verificación y validación de firmas electrónicas. Se incluyen los certificados relativos a estos servicios.

- La creación, verificación y validación de sellos electrónicos. Se incluyen los certificados relativos a estos servicios.
- La creación, verificación y validación de sellos de tiempo electrónicos. Se incluyen los certificados relativos a estos servicios.
- La entrega electrónica certificada. Se incluyen los certificados relativos a estos servicios.
- La creación, verificación y validación de certificados para la autenticación de sitios web.
- La preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

1.5.5 Autoridad de Registro (RA)

Una RA 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 RA son autoridades delegadas de la AC, Aunque es la AC en última instancia la responsable del servicio.

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

- **RA Cameral:** Aquellas gestionadas directamente o bajo el control de una Cámara de Comercio, Industria y Navegación del territorio español.
- **RA Empresarial:** Aquella gestionada por una organización pública o una entidad privada para la distribución de certificados a sus empleados.
- **RA Remota:** Autoridad de registro gestionada en una localización remota que se comunica con la plataforma mediante la capa de integración de la plataforma de gestión de AC Camerfirma - STATUS.

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

- La propia Autoridad de Certificación.
- Las Cámaras de Comercio, Industria y Navegación de España o aquellas entidades delegadas por éstas. El proceso de registro puede ser realizado por parte de diferentes entidades delegadas.
- Las Autoridades de Registro Empresariales Españolas (RA Empresarial), como entidades delegadas de una RA, a la que se vinculan contractualmente, para llevar a cabo los registros completos de Sujetos/Firmantes dentro de una determinada organización o demarcación. Con carácter general, los operadores de dichas RA 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 RA de la que dependen. Por ejemplo, los empleados de una corporación, los asociados de una agrupación empresarial, los colegiados de un colegio profesional.
- Los organismos pertenecientes a las administraciones Públicas Españolas.

- Otros agentes nacionales o internacionales que mantengan una relación contractual con la AC y supere los procesos de alta y se obligue a superar las Auditorías exigidas en las Políticas de Certificación correspondientes**.**

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

CHAMBERS OF COMMERCE ROOT - 2016	AC	Cámaras Comercio españolas	Empresa española	Administraciones Publicas española	Otros
AC CAMERFIRMA FOR NATURAL PERSONS	si	si	si	si	no
AC CAMERFIRMA FOR LEGAL PERSONS	si	si	si	si	no
AC CAMERFIRMA FOR WEBSITES	si	no	si	no	no
AC CAMERFIRMA CODESIGN	si	no	no	no	no
AC CAMERFIRMA TSA	si	no	no	no	no
GLOBAL CHAMBERSIGN ROOT - 2016					
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS	si	si	si	si	si
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS	si	si	si	si	si
AC CAMERFIRMA FOR WEBSITES	si	no	no	no	no

- **PVP.** Punto de Verificación Presencial que depende siempre de una RA. Su principal misión es la de cubrir la evidencia de la personación del solicitante y de la entrega de documentación a la RA 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 ni controles.

  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. AC Camerfirma ha elaborado un documento tipo de relación entre la RA y el PVP.

  Habida cuenta que no tiene capacidad de registro, se vinculan contractualmente con una RA mediante un contrato tipo proporcionado por Camerfirma. En base a la documentación suministrada por el PVP, el operador de la RA 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 RA en el PVP.

- **Agencia Delegada** (únicamente aplicable para AC CAMERFIRMA PERÚ): las ER pueden delegar mediante contrato, a entidades de confianza las mismas funciones que están asumiendo como ER debidamente acreditada, de cara a ofrecer el mismo servicio en zonas geográficas alejadas del domicilio de la ER. Aunque se trate generalmente de entidades con personalidad jurídica distinta de la de la ER, en su

condición de Agencia Delegada de la ER, serán objeto de control y seguimiento como si fuera una sucursal de la ER, debiendo asumir las mismas obligaciones y responsabilidades y someterse en su caso a las auditorías realizadas a la ER por el órgano de supervisión competente.

La Agencia Delegada deberá tener la capacidad necesaria para determinar la identidad, capacidad y libertad de acción de los solicitantes. Su intervención se realizará con presencia física del solicitante, cotejando documentos originales con las copias que de los mismos aporte el usuario, o con información incluida en los formularios de tramitación. En cualquier momento la ER podrá realizar auditorías internas para comprobar el cumplimiento correcto de las funciones.

La ER valorará la suficiencia de la capacidad de la Agencia Delegada en base a su prestigio, independencia y su relación previa que pueda tener con los usuarios y deberá comunicar al organismo de supervisión su creación.

1.5.6 Sujeto/Titular y Firmante.

Entendemos por Sujeto (*Subject*) al titular del certificado y viene descrito en el atributo CN (*Common Name*) del campo DN (*Distinguished Name*) del certificado. El sujeto puede ser:

- Una persona física.
- Una persona física asociada a una organización.
- Una persona jurídica.
- Un dispositivo hardware o aplicativo informático operado por o en nombre de una persona jurídica.

Cuando un Firmante sea el sujeto del certificado este será directamente responsable de las obligaciones asociadas a la gestión de dicho certificado.

Cuando un Firmante actúa en nombre de uno o varios sujetos a los cuales está ligado (ejemplo: una empresa que pide certificados para sus empleados para que actúen en nombre de la empresa).

Las conexiones entre el sujeto y el Firmante pueden ser:

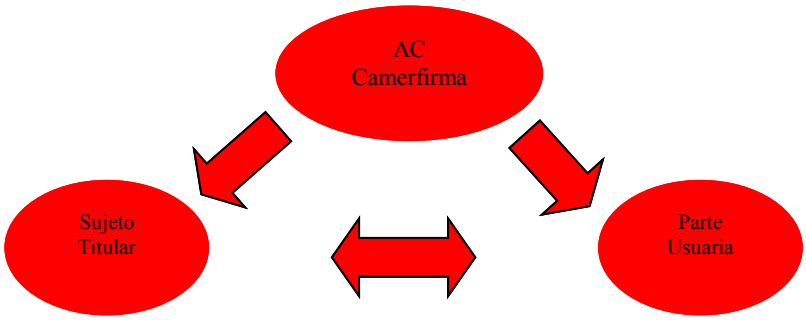
- Cuando hablamos de una persona física el Firmante puede ser:
  - La misma persona física
  - Una persona física en representación del sujeto del certificado.
  - Cualquier entidad autorizada para representar a la persona jurídica para la cual la persona es identificada en asociación al campo organización (O) del certificado.
- Cuando hablamos de una persona jurídica el Creador del Sello puede ser:
  - Cualquier entidad autorizada para representar a la persona jurídica.

    - Un representante legal.
- Cuando hablamos de un dispositivo el Firmante puede ser:
    - La persona física que opera el dispositivo o aplicativo.
    - Cualquier entidad autorizada para representar a la persona jurídica.
    - Un representante legal.

Para evitar conflicto de intereses AC Camerfirma no permite que el Firmante y la RA sean la misma entidad excepto cuando se solicita certificados para organización asociada a la RA o personas asociadas a dicha organización.

1.5.7 Parte Usuaria o usuario del certificado.

En esta CPS se entiende por Parte Usuaria 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.



1.5.8 Entidad/Organización.

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

1.5.9 Solicitante.

Bajo esta CPS se entenderá por Solicitante al Firmante.

1.5.10 Responsable de certificados /Poseedor de las claves

Para los certificados emitidos a personas físicas, esta CPS considera responsable al titular del certificado (Sujeto).

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

1.5.11 Ámbito de Aplicación y Usos.

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

Los certificados de Camerfirma podrán usarse en los términos establecidos por las Políticas de Certificación correspondientes.

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

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

1.5.11.1 Usos Prohibidos y no Autorizados.

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso 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 RA o con el firmante (sujetos) y/o Firmantes tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

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 signatario cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado. Asimismo, le será imputable al signatario 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 el firmante (sujeto), 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 constraints*)** 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*),** "restricciones de nombre" **(*name constraints*)** 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.

1.6. Normativa legal aplicable

Camerfirma viene obligada al cumplimiento de requerimientos marcados en la **legislación española y de la Unión Europea vigentes** como entidad mercantil prestadora de servicios de certificación digital (en adelante, normativa o legislación vigente). Dicha normativa queda definida en el documento interno **"Conformidad con los requerimientos legales"**.

AC Camerfirma tomará en cuenta para ofrecer sus servicios a personas discapacitadas los estándares marcados en la norma ETSI EN 301 549

1.7. Contacto

Esta CPS, está administrada y gestionada por el departamento jurídico de Camerfirma pudiendo ser contactado por los siguientes medios:

E-mail:	**juridico@camerfirma.com** Dirección Internet de datos de contacto https://www.camerfirma.com/address

2. Cláusulas Generales

2.1. Obligaciones

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 cualificados o reconocidos.
- 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.

2.1.1 AC subordinada externa.

Las AC subordinadas externas son AC 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 emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
- Permitir la auditoria anual por parte de Ac Camerfirma.
- 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.

2.1.2 RA

Las RA son las entidades delegadas por la AC para realizar las tareas de registro y aprobación de las solicitudes de certificados, por lo tanto, la RA 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 incluso en los casos de entidades delegadas por estas como son los puntos de verificación presencial.

La información sobre el uso y responsabilidades de Firmante se suministra mediante la aceptación de las cláusulas de uso previamente a la confirmación de la solicitud del certificado y mediante correo electrónico.

2.1.3 Firmante

El Firmante (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:

- Aceptar los términos y condiciones impuestas por el prestador.
- Usar la información del firmante bajo las normas impuestas por la ley de protección de datos.
- Permitir la publicación de los certificados digitales en un repositorio público.
- Suministrar a la RA 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.

2.1.4 Sujeto/Titular.

El sujeto 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 RA.
- 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 RA 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 cualificados, el Firmante 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.

Si el Firmante genera sus propias claves, se obliga a:

- Generar sus claves de Firmante utilizando un algoritmo reconocido como aceptable para la firma electrónica, en su caso cualificado, o el sello electrónico, en su caso cualificado.
- 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, en su caso cualificado, o el sello electrónico, en su caso calificado.

2.1.5 Parte Usuaria/Usuario.

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 en toda su cadena de certificación 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.
- 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.

2.1.6 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.

2.1.7 Repositorio

Camerfirma dispone de un servicio de consulta de certificados emitidos y listas de revocación. Estos servicios están disponibles públicamente en su página Web.

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. Estos servicios están disponibles públicamente en su página Web.

Esta información es custodiada dentro de una base de datos relacional con medidas de seguridad que permiten su custodia de acuerdo con las exigencias de las Políticas de Certificación correspondientes.

Camerfirma publica los certificados emitidos, las listas de revocación, políticas y prácticas de certificación de forma libre y gratuita.

Camerfirma reclama previamente la autorización del titular antes de la publicación del certificado.

2.2. Responsabilidad.

<u>La responsabilidad de Camerfirma</u>

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."

El artículo 13 del Reglamento eIDAS dispone que:

1. Sin perjuicio de lo dispuesto en el apartado 2, los prestadores de servicios de confianza serán responsables de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el presente Reglamento.

La carga de la prueba de la intencionalidad o la negligencia de un prestador no cualificado de servicios de confianza corresponderá a la persona física o jurídica que alegue los perjuicios a que se refiere el primer párrafo.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando ese prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero se produjeron sin intención ni negligencia por su parte.

2. Cuando un prestador de servicios informe debidamente a sus clientes con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

3. Los apartados 1 y 2 se aplicarán con arreglo a las normas nacionales sobre responsabilidad.

Así pues, Camerfirma será responsable de los daños y perjuicios ocasionados a los usuarios por sus servicios, ya sea al Sujeto/Firmante o a la Parte Usuaria, 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 RA.

- La garantía de que, en el momento de la entrega del certificado, obra en poder del Sujeto/Firmante, 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 éstas prácticas de certificación.

Responsabilidad de la AC subordinada (Interna/Externa).

Sin perjuicio de la responsabilidad de Camerfirma por la emisión y revocación de los certificados digitales de las propias AC subordinadas 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 Firmantes y demás terceros o usuarios afectados por el servicio de acuerdo con sus propias Declaraciones de Prácticas de Certificación, Políticas de Certificación y su legislación nacional en su caso.

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.

- Informar adecuadamente a los solicitantes de la firma de sus obligaciones y responsabilidades.
- La adecuada identificación de los solicitantes, que deben ser personas capacitadas o autorizadas para solicitar un certificado digital.
- 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 o representación.
- Acceder a la aplicación de Autoridad de Registro para gestionar las solicitudes y los certificados emitidos.

2.- Obligaciones una vez expedido el certificado.

- 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.
- El mantenimiento de los certificados durante su vigencia (extinción, suspensión, revocación).
- 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 a 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.

2.2.1 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.

Camerfirma y las RAs tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y en las Políticas de Certificación
3. Por el uso indebido o fraudulento de los certificados o CRLs emitidos por la AC
4. Por el uso de la información contenida en el Certificado o en la CRL.
5. Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
6. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
7. Por la no recuperación de documentos cifrados con la clave pública del Sujeto.

2.2.2 Límite 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.

2.3. Responsabilidad financiera

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**.

2.4. Interpretación y ejecución

2.4.1 Legislación

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.

2.4.2 Independencia

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

2.4.3 Notificación

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

2.4.4 Procedimiento de resolución de disputas.

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

2.5. Tarifas

2.5.1 Tarifas de emisión de certificados y renovación.

Los precios de los servicios de certificación o cualquier otro servicio relacionado 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 de venta al público, excepto aquellos que están sujetos a una negociación comercial previa.

2.5.2 Tarifas de acceso a los certificados.

El acceso a los certificados emitidos es gratuito, no obstante, 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 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.

2.5.3 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 a través de listas de certificados revocados o mediante acceso vía Web en la dirección Internet de Camerfirma http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

El servicio OCSP se ofrece de forma gratuita.

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

El acceso al contenido de la presente CPS es gratuito.

2.5.5 Política de reintegros.

AC Camerfirma no tiene una política de reintegros específica, y se acoge a la normativa general vigente.

2.6. Publicación y repositorios.

2.6.1 Publicación de información de la AC.

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 y las PDS correspondientes (*PKI Disclosure Statement*).

- Los instrumentos jurídicos vinculantes con firmantes 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

AC Camerfirma no retirará la versión anterior del documento objeto del cambio, indicando que ha sido sustituido por la versión nueva.

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

2.6.1.1 Políticas y Prácticas de Certificación.

La presente CPS y Políticas actuales están disponibles públicamente en el sitio de Internet: https://policy.camerfirma.com.

Las políticas de certificación de AC subordinadas también estarán publicadas o referenciadas en el sitio internet de AC Camerfirma.

2.6.1.2 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 de condiciones antes de proceder a la solicitud.

Cuando el sujeto/firmante acepta los términos y condiciones in 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.

2.6.1.3 Difusión de los certificados.

Se podrá acceder a los certificados emitidos, siempre **que el Sujeto/Firmante dé 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 Firmante. La respuesta del sistema, si encuentra un Firmante con

ese email, es una página con todos los certificados asociados ya estén activos, caducados, o revocados. De esta forma la consulta no permite descargar certificados de forma masiva.

2.6.2 Frecuencia de publicación.

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

AC Camerfirma emite y publica **listas de revocados** de forma periódica siguiendo la tabla marcada en el apartado correspondiente de estas prácticas de certificación: **"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.

AC Camerfirma podrá retirar la referencia al cambio de la página principal al cabo de 15 (quince) días desde la publicación de la nueva versión y se insertaría en el depósito correspondiente. Las versiones antiguas de la documentación son conservadas al menos por un periodo de **15 (quince) años,** pudiendo ser consultadas, con causa razonada por los interesados.

2.6.3 Controles de acceso a los repositorios.

Camerfirma publica los certificados y CRLs 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.
- El solicitante autoriza o no a la publicación de su certificado en el proceso de solicitud.

2.7. Auditorías

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 sujeta a unas auditorías periódicas con el sello ***WEBTRUST for CA***, ***WEBTRUST SSL BR*** y ***WEBTRUST SSL EV*** que asegura que los documentos de políticas y CPS tienen un formato y alcance adecuado a la vez que están completamente alineadas con su políticas y prácticas de certificación.

Para la adecuación de conformidad eIDAS, AC Camerfirma realiza una evaluación de conformidad bienal tal como marca el reglamento de las siguientes normas: **EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 421.**

Las **Autoridades de Registro** 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 auditorías se describen en un "Plan Anual de Auditorías".

AC Camerfirma está sujeta a una auditoria bienal sobre LOPD.

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 evidencia recogidas sean correctas y suficientes para la emisión del certificado.

2.7.1 Frecuencia de las auditorías

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**, ciclo de 3 años con revisiones anuales.
- **WEBTRUST for CA, WEBTRUST SSL BR, WEBTRUST SSL EV** de forma anual.
- Evaluación de conformidad **eIDAS**, bienal con revisión anual
- Auditoria **LOPD**, bienal con revisión anual.
- Auditorías **RA** de forma discrecional.
- Auditorías **Internas**, AC subordinadas Externas, TSU Externas, de forma discrecional.

2.7.2 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 la auditoria WEBTRUST - AUREN http://www.auren.com.
- Para las auditorías ISO27001/20000 -AENOR. http://www.aenor.es/aenor/inicio/home/home.asp
- Para las auditorías internas / RA / AC subordinada, TSA LOPD – AUREN http://www.auren.com/
- Para la evaluación de conformidad eIDAS Natural Person & Legal Person. – TÜVIT https://www.tuvit.de/en/
- Para la evaluación de conformidad eIDAS Sellos de tiempo y Certificados Website CSQA https://www.csqa.it/

2.7.3 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.

2.7.4 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 Camerfirma cumple con los requerimientos de las Políticas de Certificación que gobiernan la emisión de los distintos certificados digitales.
c) 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.
d) Que Camerfirma gestiona de forma adecuada la seguridad de sus sistemas de información.
e) En los certificados de OV y EV la auditoría comprueba la alienación con las políticas marcadas por CABFORUM tanto en las "*Baseline Requirements*" como "*EV SSL Certificate guidelines*".

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

- Procesos de Camerfirma, RAs y elementos relacionados en la emisión de certificados sellos de tiempo TSA 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

2.7.5 Auditorías de AC subordinada Externa.

AC Camerfirma a través de sus auditores realiza una auditoria anual a las organizaciones que han obtenido un certificado de AC subordinada 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 for CA*** y/o ***WebTrust for EV*** según corresponda a los certificados emitidos.

2.7.6 Auditoria en las Autoridades de Registro

Todas las RA son auditadas. Estas auditorías se realizan al menos cada dos años de forma discrecional y en base a un análisis de riesgos. Las auditorías 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 RA son:

IN-2010-04-12-Procedimiento de Evaluación de la Seguridad en RA
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 RA.
IN-2010-04-17-Informe de evaluación

2.7.7 Tratamiento de los informes de auditoría

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.

2.8. Confidencialidad

2.8.1 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.

Camerfirma cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos. En este sentido, este documento sirve, de conformidad con la Ley 59/2003, de Firma Electrónica (artículo 19.3) como documento de seguridad.

Documentación de referencia:

IN-2006-05-11-Conformidad de Requerimientos legales

2.8.2 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.

2.8.3 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.

2.8.4 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.

2.9. 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.

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Tipos de nombres

El Sujeto/Titular del certificado se describe en este 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://webcrm.camerfirma.com/incidencias/incidencias.php.

La estructura y el contenido de los campos de cada certificado emitido por Camerfirma, así como su significado semántico se encuentran descritos en cada uno 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:** En certificados correspondientes a **personas jurídicas**, esta identificación se realizará por medio de su denominación o razón social, y su identificación fiscal.
- **Componentes o dispositivos:** Los certificados **de entidad final que describen componentes o dispositivos** incorporan un nombre identificativo de la máquina o servicio, adicionalmente la entidad jurídica propietaria de dicho servicio en el campo organización "O" del "CN".
  - La estructura para los certificados de **AC subordinada, TSU, TSA, 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)
  - El certificado de **Servidor Seguro** incluye dependiendo del tipo de certificado el dominio FQDN (*Fully Qualified Domain Name*) sobre el cual la organización "O" descrita en el certificado tiene propiedad y control.
  - 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 Pseudónimos

La admisión o no de pseudónimos es tratada en cada una de las Políticas de certificación. En caso de ser aceptados Camerfirma utilizara el Seudónimo en el atributo CN del nombre del Sujeto/Firmante guardando confidencialmente la identidad real del Sujeto/Firmante.

El cálculo del seudónimo en aquellos certificados donde se permita, se realiza de manera que se identifica unívocamente al titular real del certificado**.**

3.1.3 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.

3.1.4 Unicidad de los nombres

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

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

Bajo esta CPS un Firmante puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

CIF. Identificador fiscal de la empresa
NIF. Identificador fiscal de la persona física
Tipo de Certificado (OID de identificador de política de certificación).
Soporte del certificado. (Software, Tarjeta, Nube)

Como excepción esta CPS permite emitir un certificado cuando coincida CIF, NIF, Tipo, soporte, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, en los campos cargo (*title*) y/o departamento (*organizationalUnit*).

3.1.5 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.

Camerfirma en todo caso se atiene a lo dispuesto en el apartado 2.4.4 de esta CPS.

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 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.

3.1.7 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.

El modelo de generación de claves utilizado viene indicado en el propio certificado, tanto en su identificador de Política como en el atributo Descripción del campo DN del certificado. Estos códigos están descritos en las Políticas correspondientes y en las fichas de perfiles de los certificados.

a) Generación de claves por parte de Camerfirma.

   En Software: Se entregan al Firmante en mano o mediante correo mediante 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 este en las aplicaciones, es entregada por un medio distinto al utilizado en la recepción del fichero (correo electrónico, teléfono)

   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).

b) Generación de las claves por el Firmante.

   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**.

3.1.8 Autenticación de la identidad de un individuo, la entidad y su vinculación.

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 RA, exige:

3.1.8.1 En los certificados para operador de RA (Persona Física).

- Se comprueba que el solicitante ha superado el examen de operador
- 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 de la organización
- El dominio del email asociado al certificado es un mail de la organización.

3.1.8.2 En los Certificados cualificados.

Aquellos así descritos bajo el reglamento eIDAS (REGLAMENTO (UE) Nº 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.

3.1.8.2.1 Identificación del Sujeto/Firmante.

Se exige la personación física (o sus alternativas según describe en eIDAS) del Sujeto o Firmante cuando éste sea también Solicitante o de un representante del Solicitante cuando éste es una entidad jurídica, presentando alguno de los siguientes documentos:

- Documento Nacional de Identidad.
- Tarjeta de residencia.
- Pasaporte.
- Documento de identidad apostillado para solicitantes fuera del territorio español

La presencia física no es obligatoria en estos certificados en los casos que marca eIDAS.

http://www.camerfirma.com/index/buscador-documentos.php

En el caso de representante del Sujeto/Firmante, presentación de una autorización firmada por un representante de la entidad que actuará como Solicitante.

En el caso de entidades fuera del territorio español se entregará el documento acreditativo de la capacidad de representación de la persona firmante de la autorización debidamente apostillada, para poder comprobar la veracidad de la documentación.

3.1.8.2.2 Identidad del servicio o máquina

.

El uso de IPs y dominios privados/locales esta prohibido después de octubre de 2016. Camerfirma dejó de emitir certificados de este tipo el 1 de noviembre de 2016. En cualquier caso, los certificados emitidos de este tipo se revocan si su fecha de vencimiento es posterior a octubre de 2016.

La información del dominio se tomará del servicio WHOIS del registrador del dominio para el cual se aplican las reglas marcadas por su correspondiente ccTLD o gTLD. Se comprueba mediante el acceso a las bases de datos de dominios Internet WHOIS:

- http://www.internic.net/whois.html
- http://www.networksolutions.com
- http://en.gandi.net
- http://www.interdomain.es
- https://www.nic.es/ (.es)
- http://www.eurid.eu/ (.eu)
- http://www.nic.coop/whoissearch.aspx (.coop)
- http://www.nominalia.com/
- http://www.arsys.es/

Cuando la solicitud de emisión sea para un certificado de servidor seguro o de sede electrónica Camerfirma examinará el registro de la ACs autorizadas, CAA, según la RFC 6844, y si esos registros CAA están presentes y no permiten a Camerfirma emitir esos certificados porque no se encuentra registrado, Camerfirma no emitirá ese certificado pero permitirá a los solicitantes volver a realizar la solicitud una vez se haya podido subsanar esta situación. El cliente deberá modificación los datos de su dominio para permitir a Camerfirma emitirle dicho certificado.

La herramienta a utilizar para comprobar la asignación del prestador al dominio será https://toolbox.googleapps.com/apps/dig/#ANY/

3.1.8.2.3 Identificación de la entidad.

Con carácter previo a la emisión y entrega de un certificado de organización es necesario autenticar los datos relativos a la constitución y la personalidad jurídica de la entidad. Se exige la identificación de la entidad, para lo que la RA requerirá la documentación pertinente en función del tipo de entidad. Esta información se publica en los Manuales operativos de la RA y en la página web de Camerfirma.

http://www.camerfirma.com/index/buscador-documentos.php

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

En la emisión de certificados de componente SSL OV/EV La existencia de la entidad se comprueba mediante el acceso a los registros públicos (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es), Informa (www.informa.es) o a las bases de datos de la Agencia tributaria (www.aeat.es). En **EV** Debe comprobarse fehacientemente la actividad operativa de la entidad. Esta comprobación se realizará mediante el acceso al registro mercantil o mediante la consulta a otros registros de actividad empresarial del mercado. En el caso de entidades fuera del territorio español la documentación que deben aportar será la del Registro Oficial del país correspondiente debidamente apostillada donde se indique la existencia de la entidad en dicho país, además:

- La comprobación de que los datos o documentos aportados no tengan una antigüedad superior a **1 año**.
- Consulta de la antigüedad mínima de existencia legal de la organización de **1 año.**
- No se podrá emitir certificados a empresas erradicadas en países donde exista una prohibición gubernamental para hacer negocios.

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.

3.1.8.2.4 Identificación de la vinculación.

Tipo de certificado	Documentación
Representante de Persona Jurídica con Poderes Generales de Representación. Representante de entidad sin Personalidad Jurídica con Poderes Generales de Representación. Representante de Persona Jurídica para trámites con las AAPP	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

Tipo de certificado	Documentación
Representante de Entidad sin Personalidad Jurídica para trámites con las AAPP Representante de Persona Jurídica para Apoderados Representante de Entidad sin Personalidad Jurídica para Apoderados	de la RA y en la página web de Camerfirma.
Corporativos	En general, autorización firmada por un representante legal o apoderado general de la entidad
Sello electrónico	Autorización para solicitar el certificado de por alguien con poder de representación suficiente de la entidad firmante. Certificado o consulta al Registro Mercantil para comprobar la constitución, personalidad jurídica de la entidad y el nombramiento y vigencia del cargo del autorizante.
Empleado público/ Sede y Sello	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 ésta persona

Servidor	Control del dominio por parte de la entidad Firmante. Camerfirma comprueba que los datos obtenidos en la consulta al servicio WHOIS Internet coinciden claramente con los datos de la entidad presentados en la solicitud Puede producirse que el dominio este asignado en la base de datos del registrador a un tercero encargado de su gestión. En dicho caso para que aparezcan los datos del titular último del dominio en el certificado, se necesitara: 1. Una autorización de éste para la emisión del certificado. 2. Una comunicación de la organización o persona que controla el registro del dominio indicando esta circunstancia. Para los certificados de EV Las Guías de emisión de certificados exigen la diferenciación de tipos de organización diferentes (Privadas, Gobierno, Negocio). En estos casos, la solicitante marca en el documento de solicitud el tipo de entidad a la que pertenece. La autoridad de registro verificará su exactitud. El certificado incorporará dicha información tal y como se define en las políticas de certificación de referencia. En los certificados emitidos con extensión SAN (*Subject Alternative Name*). Los procedimientos antes mencionados deben ejecutarse para cada uno de los dominios incorporados en el certificado, no pudiéndose emitir el certificado sin alguno de ellos no cumple los requisitos marcados.

Tipo de certificado	Documentación
Firma de código	Autorización para solicitar el certificado de por alguien con poder de representación suficiente de la entidad firmante. Certificado o consulta al Registro Mercantil para comprobar la constitución, personalidad jurídica de la entidad y el nombramiento y vigencia del cargo del autorizante.
TSU	Autorización para solicitar el certificado de por alguien con poder de representación suficiente de la entidad firmante. Certificado o consulta al Registro Mercantil para comprobar la constitución, personalidad jurídica de la entidad y el nombramiento y vigencia del cargo del autorizante.

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

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.

3.1.8.4 Consideraciones en la identificación usuarios y vinculación en al AAPP.

Existen aspectos a considerar respecto las autoridades de registro establecidas en la administración pública y operadas por empleados públicos, teniendo estos últimos consideración de notarios 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.

3.1.8.5 Consideraciones especiales para la emisión de certificados fuera de territorio español.

Aspectos que tiene que ver con la documentación de identidad de las personas física, 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.

- PERU
- ANDORRA
- COLOMBIA
- MEXICO
- UK
- FRANCIA

3.2. Renovación de la clave

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

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.

En el caso de renovación de los **certificados cualificados 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.

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 en la página Web de Camerfirma http://www.camerfirma.com/area-de-usuario/renovacion-de-certificados/. Este proceso requiere disponer del certificado válido (no revocado) 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.

Para los certificados técnicos, es decir servidor seguro, sello empresarial y firma de código no se permite la renovación, debiéndose realizar el proceso correspondiente a una emisión nueva.

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 año siempre y cuando no haya constancia de que ha dejado de ser Operador de RA.

Los certificados de **TSU**, se emiten con una duración de 6 años y un uso de la clave privada de 1 año, por lo que se renuevan anualmente.

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.

3.3. Reemisión después de una revocación

Al quedar el certificado invalidado no se podrá realizar la renovación automatizada. El solicitante deberá iniciar un proceso de emisión nueva.

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. Renovación de certificados sin renovación de claves

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

3.5. Renovación de certificados con renovación de claves

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

3.6. 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 Firmante 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 en lugar de la modificación con revocación previa del certificado a modificar.

3.7. Solicitud de revocación

La forma de realizar las solicitudes de revocación se establece en el apartado 4.8 de este documento.

4. Requerimientos Operacionales

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 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 Firmante 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.

Las solicitudes de certificados de AC subordinada, TSA deben realizarse formalmente a través de la solicitud de una oferta comercial y posteriormente incorporada en los formularios de solicitud de la plataforma STATUS.

4.1.2 Lotes.

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

4.1.3 Solicitudes de certificados de entidad final en HSM, TSU y AC subordinada.

Las solicitudes para la emisión de certificados en HSM, TSU o AC subordinada 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 prácticas 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 Firmantes 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 RA al expediente documental soporte para la emisión del certificado.

Para cada tipo de certificado el Firmante debe aceptar los términos y condiciones de uso entre el Firmante, la autoridad de registro y la autoridad de certificación. Este proceso se realiza bien mediante la firma manuscrita de un contrato, bien mediante una aceptación de términos visualizados en una página Web antes de proceder a la creación y descarga del certificado.

4.1.4 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, 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 "ciega" de 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 auditorías 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 y esta declaración de prácticas de certificación bajo la que se rigen.

4.1.5 Procesamiento de la solicitud de certificación

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.

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 se presente con la documentación correspondiente.

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.

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

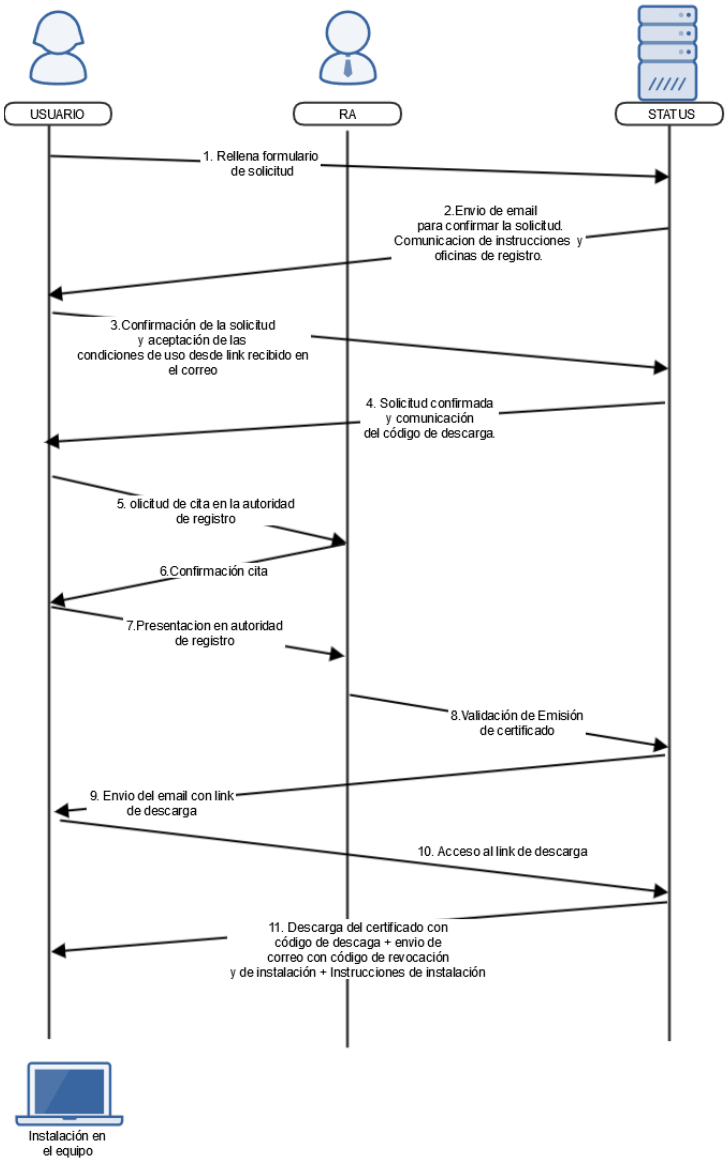
4.2. Petición de certificación cruzada.

Camerfirma no tiene actualmente ningún proceso de certificación cruzada activo.

4.3. Emisión de certificados

4.3.1 Certificados en Software:

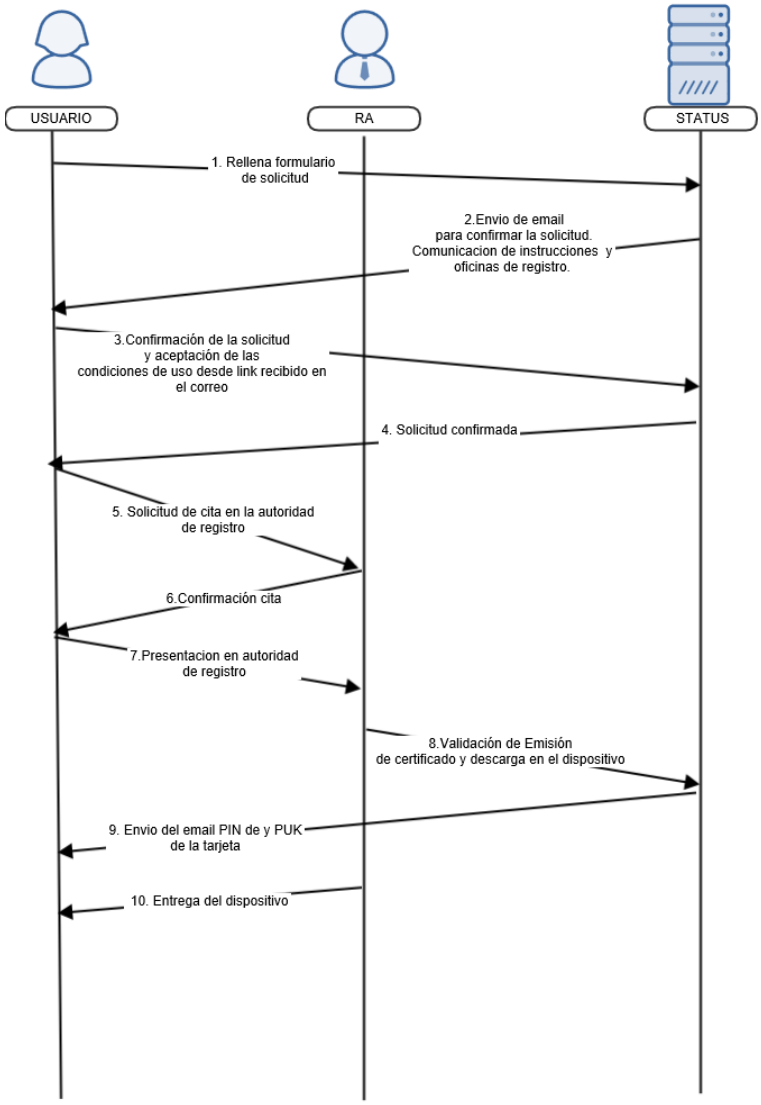
Una vez aprobada la solicitud el Firmante recibe un correo electrónico con la notificación de este hecho y con el Proceder a la generación y descarga del certificado. Para su instalación necesitara del código de producto que le ha sido entregado con el contrato y un código de instalación que se habrá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



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

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

4.3.2.1 En Tarjeta o Token Criptográfico.



El usuario recibe en las dependencias de la RA 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 Camerfirma admite varios tipos de tarjetas y tokens USB todos ellos previamente certificados DSCF (Dispositivo seguro de creación de firma).

Para las tarjetas por defecto (distribuidas por Bit4Id) el Firmante 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 tarjetas la gestión de PIN/PUK está fuera del alcance de este documento.

4.3.2.2 Peticiones vía WS:

Las solicitudes pueden ser recibidas mediante llamadas convenientemente firmadas a la capa de servicios del WS de la aplicación STATUS según apartado 4.1.4.

4.3.3 Certificado de servidor seguro EV

El **Certificado de servidor seguro EV**, requiere, según las políticas específicas de este tipo de certificado, la presencia física del solicitante o de un tercero debidamente acreditado. El administrador de la RA verifica el pago del servicio, la documentación relativa a la petición y la identidad del Sujeto/Firmante.

Las políticas de certificación para la emisión de certificados de SSL EV a las que se adhiere esta CPS ("*CA/Browser Forum Guidelines for Issuance and Management of extended validation certificates*"), exigen que cada petición de emisión de un certificado EV, sea aprobada por dos personas distintas. El procedimiento seguido en la validación de estos certificados garantiza la verificación doble de la siguiente forma:

- Validación por parte del operador de la red de registro de los datos administrativos como la presencia física la entrega de documentación y autorizaciones.

- Una vez pasado este trámite el departamento de operaciones de AC Camerfirma revisa esta documentación y procede a la validación definitiva y la emisión del certificado.

El Firmante, puede realizar con sus propios medios, la generación de las claves en un dispositivo criptográfico y entregar la petición en formato PKCS#10 a Camerfirma para emitir el certificado. En el caso de que el certificado fuera emitido bajo formato hardware con dispositivo HSM se pedirá una evidencia de este hecho tal como se describe en el punto 4.1.3 de este documento.

Si la clave privada es generada por Camerfirma, una vez aprobada la petición por el operador de RA, se le hará llegar al Sujeto/Firmante:

- ✓ Un link a la página donde se generará el certificado en formato PKCS#12.
- ✓ Una contraseña necesaria para la instalación de las claves y el certificado en el equipo del firmante.
- ✓ El Sujeto/Firmante necesitara también para el proceso de obtención de las claves y el certificado, un código de descarga se suministra por el aplicativo en el proceso de solicitud.

Si la clave es generada por el Firmante, Camerfirma enviara al usuario un certificado en formato PKCS#7.

4.3.4 Certificado de cifrado.

Bajo estas prácticas de certificación los certificados exclusivamente de cifrado se emiten para empleados de la administración pública en su nivel alto.

4.3.5 Certificados de AC subordinada:

Las emisiones de certificados de AC subordinada se realizan en una ceremonia de emisión de certificado de AC subordinada, en las instalaciones de AC Camerfirma en un entorno de seguridad y bajo la supervisión de un auditor interno.

4.3.6 Certificados de TSU:

Las emisiones de certificados de TSU se realizan en una ceremonia de emisión de certificados en un entorno de seguridad por personal confiable.

4.4. Aceptación de certificados.

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.

4.5. Notificación de la emisión a los interesados

En los certificados de entidad final emitidos por Camerfirma se produce una notificación mediante un correo electrónico al solicitante indicando la aprobación o denegación de la solicitud.

Los certificados de entidad intermedia o raíz se emiten bajo la ejecución de una ceremonia de claves y son posteriormente entregados al titular del certificado.

4.6. Publicación del certificado

Los certificados emitidos son publicados en la siguiente dirección http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/

Camerfirma distribuye sus certificados de Root en su página web:
http://www.camerfirma.com/area-de-usuario/descarga-de-claves-publicas/

Camerfirma distribuye sus certificados de AC subordinada en su página web:

http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

Camerfirma distribuye sus certificados de OCSP en su página web:
http://www.camerfirma.com/servicios/respondedor-ocsp/

Camerfirma distribuye sus certificados de TSA en su página web:
http://www.camerfirma.com/servicios/sellado-de-tiempo/

4.7. Notificación de la emisión a terceros

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 Trasparency*".**

4.8. Suspensión y revocación de certificados.

4.8.1 Aclaraciones previas

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). Se revoca un certificado de forma cautelar hasta que se decida sobre la oportunidad o no de realizar una revocación con causa definitiva o su activación.

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).

Los motivos de suspensión de un certificado vienen definidos en la política de certificación concreta.

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 bajo estas prácticas la reinstalación 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.

4.8.2 Causas de revocación y documentos justificativos

Las causas de revocación de un certificado vienen definidas en su política de certificación concreta.

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, así como la finalidad de la autorización del Firmante al responsable del certificado o la finalización de la relación entre Firmante 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 estas 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 persona jurídica, 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.

4.8.3 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 RA 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.

- Camerfirma puede, en caso de que localice un error en el certificado, revocarlo de manera unilateral en un plazo máximo de 1 semana. Dependiendo de la gravedad y en caso de que la seguridad del usuario pueda estar comprometida el prestador podrá de forma unilateral revocar el certificado en 24 horas.

Adicionalmente las que marquen las políticas de certificación concretas.

4.8.4 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 RA en horario de atención al público mostrando el **DNI** del Sujeto/Firmante 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 AC subordinada y TSU.

- ✓ Para los certificados de **servidor seguro, sello de empresa o certificado de firma de código** puede solicitarse a través del correo desde el cual se solicitó la emisión del certificado enviando la solicitud a gestión_soporte@camerfirma.com. El operador de Camerfirma confirmará telefónicamente la solicitud de revocación para darle curso.

Camerfirma mantiene en su página Web toda la información relativa a los procesos de revocación de los certificados. http://www.camerfirma.com/area-de-usuario/revocacion-de-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 del precio del certificado emitido, 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.

4.8.5 Periodo de revocación

Para los certificados de entidad final. El periodo de revocación desde que Camerfirma o una RA 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.

4.8.6 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 con causa desconocida.*

En el caso de producirse una suspensión del certificado, se envía un comunicado mediante email al Sujeto/Firmante 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 Sujeto/Firmante recibirá un correo indicando el nuevo estado del certificado.

El proceso de suspensión no se aplica a certificados

- De TSU/TSA
- De AC y AC subordinada
- De Operador de RA.

Procedimiento para la 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 Firmante debe poseer el código de revocación para proceder a la suspensión del certificado.

4.8.7 Límites del periodo de suspensión

Un certificado no permanecerá suspendido más de **una semana**.

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

4.8.8 Frecuencia de emisión de CRLs

CA	Frecuencia de emisión días	Duración días
CHAMBERS OF COMMERCE ROOT – 2016	Máximo 365	365
AC CAMERFIRMA FOR NATURAL PERSONS – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA FOR LEGAL PERSONS – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA FOR WEBSITES – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA CODESIGN – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA TSA – 2016	Inmediato - Máximo 1	2
GLOBAL CHAMBERSIGN ROOT – 2016	Máximo 365	365
AC CAMERFIRMA – 2016	Máximo 365	365
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA GLOBAL FOR WEBSITES – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA COLOMBIA – 2016	Máximo 365	365
AC CITISEG – 2016	Inmediato - Máximo 1	2
AC CAMERFIRMA PERÚ – 2016	Máximo 365	365
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016	Inmediato - Máximo 1	2

4.8.9 Requisitos de comprobación de CRLs

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. No obstante, se emitirá una nueva CRL cada vez que exista una revocación.

4.8.10 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

http://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 http://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**.

4.8.11 Requisitos de la comprobación on-line de la revocación

Para realizar la comprobación de una revocación la Parte Usuaria deberá conocer el e-mail asociado al certificado que se desea consultar si se realiza mediante acceso Web.

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

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

4.8.12 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/

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

No estipulado

4.8.14 Requisitos especiales de revocación por compromiso de las claves

No estipulado

4.9. Procedimientos de Control de Seguridad

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

4.9.1 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 en las infraestructuras que dan soporte a la emisión y gestión de certificados

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.

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.

4.9.2 Periodos de retención para los registros de auditoria

Camerfirma almacena la información de los registros de auditoría al menos durante 1**5 años**.

4.9.3 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.

4.9.4 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.

4.9.5 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.

4.9.6 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.

4.9.7 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 de Análisis de riesgos con código **CONF-2005-05-01**. 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.

4.10. Archivo de registros

4.10.1 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 y OCSP
- ✓ 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.

4.10.2 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 **15 años**.

Las versiones antiguas de la documentación también son conservadas, por un periodo de 15 (quince) años por AC Camerfirma, pudiendo ser consultadas, por causa razonada por los interesados.

4.10.3 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-** ***backup management***

4.10.4 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-** ***backup management***

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.

4.10.5 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**

4.10.6 Sistema de recogida de información de auditoria

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

4.10.7 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

4.11. 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 AC (**Root CA, AC subordinada**). 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…) lo requiera.

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

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

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.

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

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.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de Camerfirma para implementar dichos procesos.

Camerfirma como parte de su implantación de sistemas ISO27001 e ISO20000 ha desarrollado planes y procedimientos de mejora continua de forma que refuercen sistema todas aquellas experiencias recogidas en la gestión de incidencias y eviten la repetición de estas.

Documento relacionado **IN-2007-02-08 Procedimiento de mejora continúa**

4.12.1 La clave de una entidad se compromete

El Plan de contingencias enmarcado en la certificación UNE-ISO/IEC 27001 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 Sujetos/Firmantes, Parte Usuaria 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.

4.12.2 Instalación de seguridad después de un desastre natural u otro tipo de 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 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.

4.13. Cese de la AC

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 Sujetos/Firmantes, Partes Usuarias y otras ACs con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de **6 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 registros de auditoría durante el periodo de tiempo indicado a los Firmantes 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 plan de continuidad y disponibilidad de AC Camerfirma SA, apartado “Plan de Cierre”.

5. Controles de Seguridad Física, Procedimental y de Personal

Camerfirma está sujeta a las validaciones anuales de la norma UNE-ISO/IEC 27001 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 anti-humedad, 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 los elementos más críticos del sistema se realiza a través de tres zonas previas de paso con acceso limitado incrementalmente.

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 Protección y prevención 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 Copia de respaldo externa

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. Se encarga de acceder a los datos de administración de las plataformas de servicios.

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

Especialista de validación:
Las tareas del especialista de validación se centran en la validación de solicitudes de certificados de SSL/TSL en sus distintas modalidades, afecta también a los certificados de Sede electrónica para las AAPP.

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.

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 Arranque y parada del sistema de gestión PKI.

El sistema de PKI se compone de los siguientes módulos:

Módulo de Gestión de RA, 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 RA
- 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 de seguridad de personal

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

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 RA es confiable y pertenece a una Cámara de Comercio o del organismo delegado para realizar las tareas de registro.

El Administrador de RA 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-2008-00-06 Formato de Perfil Profesional

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.

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

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.

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 para albergar 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 AC subordinadas se genera en equipos HSM certificados **FIPS 140-2, en su nivel 3** donde se albergarán para su correspondiente uso. El certificado emitido por la clave raíz se realiza en una sala criptográfica segura.

CA	Longitud de claves	Algoritmo de firma	Año creación	Caducidad
CHAMBERS OF COMMERCE ROOT - 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/04/2040
AC CAMERFIRMA FOR NATURAL PERSONS – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CAMERFIRMA FOR LEGAL PERSONS – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CAMERFIRMA FOR WEBSITES - 2016	4.096 bits	sha256WithRSAEncryption	2.016	13/03/2040
AC CAMERFIRMA CODESIGN – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CAMERFIRMA TSA – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
GLOBAL CHAMBERSIGN ROOT – 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/04/2040
AC CAMERFIRMA – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS – 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/02/2040
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS – 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/02/2040
AC CAMERFIRMA GLOBAL FOR WEBSITES – 2016	4.096 bits	sha256WithRSAEncryption	2.016	12/02/2040
AC CAMERFIRMA COLOMBIA – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/03/2040
AC CITISEG – 2016	4.096 bits	sha256WithRSAEncryption	2.016	08/02/2040
AC CAMERFIRMA PERÚ – 2016	4.096 bits	sha256WithRSAEncryption	2.016	10/03/2040
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016	4.096 bits	sha256WithRSAEncryption	2.016	09/02/2040

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 Firmante

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

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

La plataforma de gestión 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 de RA remota usando la capa de servicios WEB para la solicitud PKCS#10 y la recogida del PKCS#7 correspondiente.

Las claves tienen una longitud mínima de **2048 bits**.

6.1.2 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 **PKCS#10**.

6.1.3 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

http://www.camerfirma.com/area-de-usuario/descarga-de-claves-publicas/

6.1.4 Tamaño y periodo de validez de las claves del emisor

Ver apartado 6.1.1

6.1.5 Tamaño y periodo de validez de las claves del Firmante

Las claves privadas del Sujeto/Firmante 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.

6.1.1 Parámetros de generación de la clave pública.

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

6.1.2 Comprobación de la calidad de los parámetros

Tamaño de claves = mínimo 2.048 bits
Algoritmo de generación de claves: rsagen1
Método de relleno: emsa-pkcs1-v1_5
Funciones criptográficas de Resumen: SHA-256

6.1.3 Hardware/software de generación de claves

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

Las claves de **ROOT** utilizan un dispositivo criptográfico que cumple las especificaciones **FIPS 140-2 nivel 3**.

6.1.4 Fines del uso de la clave

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

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 - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:2
Certificado Cualificado de Ciudadano	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

Certificado Cualificado Corporativo	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Representante de Persona Jurídica con Poderes Generales de Representación	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica con Poderes Generales de Representación	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Representante de Persona Jurídica para trámites con las AAPP	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica para trámites con las AAPP	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Representante de Persona Jurídica para Apoderados	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Representante de Entidad Sin Personalidad Jurídica para Apoderados	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Empleado Público de Firma. Nivel Alto.	critical, contentCommitment	-	critical,CA:false
Certificado de Empleado Público de Autenticación. Nivel Alto.	critical, digitalSignature	emailProtection clientAuth	critical,CA:false
Certificado de Empleado Público de Cifrado. Nivel Alto.	critical, keyEncipherment, dataEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Empleado Público. Nivel Medio.	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Empleado Público con Seudónimo de Firma. Nivel Alto.	critical, contentCommitment	-	critical,CA:false
Certificado de Empleado Público con Seudónimo de Autenticación. Nivel Alto.	critical, digitalSignature	emailProtection clientAuth	critical,CA:false
Certificado de Empleado Público con Seudónimo de Cifrado. Nivel Alto.	critical, keyEncipherment, dataEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Cualificado de Empleado Público con Seudónimo. Nivel Medio.	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA FOR LEGAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:2
Certificado Cualificado de Sello Electrónico	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Sello Electrónico	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Sello Electrónico AAPP. Nivel Alto.	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Sello Electrónico AAPP. Nivel Medio.	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

AC CAMERFIRMA FOR WEBSITES - 2016	critical, cRLSign, keyCertSign	serverAuth	critical,CA:true, pathlen:2
Certificado de Website OV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
Certificado Cualificado de Website EV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
Certificado Cualificado de Sede Electrónica - Nivel Alto - EV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
Certificado Cualificado de Sede Electrónica - Nivel Medio - EV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
Certificado Cualificado de Sede Electrónica - Nivel Medio - OV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
Certificado Cualificado de Sede Electrónica - Nivel Medio - OV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
AC CAMERFIRMA CODESIGN – 2016	critical, cRLSign, keyCertSign	codeSigning	critical,CA:true, pathlen:2
Certificado Cualificado de Firma de Código	critical, digitalSignature	codeSigning	critical,CA:false
Certificado Cualificado de Firma de Código EV	critical, digitalSignature	codeSigning	critical,CA:false
AC CAMERFIRMA TSA - 2016	critical, cRLSign, keyCertSign	timeStamping	critical,CA:true, pathlen:2
Certificado Cualificado de TSU	critical, contentCommitment	critical,timeStamping	critical,CA:false
Certificado de TSU	critical, contentCommitment	critical,timeStamping	
GLOBAL CHAMBERSIGN ROOT - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true
AC CAMERFIRMA - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
AC CAMERFIRMA GLOBAL FOR NATURAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:1
Certificado de Ciudadano	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado Corporativo	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Representante de Persona Jurídica	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Representante de Entidad Sin Personalidad Jurídica	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA GLOBAL FOR LEGAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:1
Certificado de Sello Electrónico	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA GLOBAL FOR WEBSITES - 2016	critical, cRLSign, keyCertSign	serverAuth	critical,CA:true, pathlen:1
Certificado de Website EV	critical, digitalSignature, keyEncipherment	serverAuth	critical,CA:false
AC CAMERFIRMA COLOMBIA - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
AC CITISEG - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:1

Certificado de Comunidad Académica	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Función Pública	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Persona Jurídica	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Persona Natural	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Pertenencia a Empresa	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Profesional Titulado	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Representante de Empresa	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
AC CAMERFIRMA PERÚ - 2016	critical, cRLSign, keyCertSign	-	critical,CA:true, pathlen:2
AC CAMERFIRMA PERÚ CERTIFICADOS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true, pathlen:1
Certificado de Persona Física con Vinculación a Empresa	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Representante Legal	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Persona Jurídica	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
Certificado de Facturación Electrónica	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	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.

6.2. Protección de la clave privada

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**.

Clave privada del Firmante

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

Cuando se almacene en formato software Camerfirma ofrece instrucciones de configuración para un uso seguro.

Respecto a los dispositivos criptográficos distribuidos por Camerfirma para albergar certificados cualificados, cumplen todos con los requisitos de dispositivos seguros de creación de firma cualificados y por lo tanto son aptos para la generación de firma cualificada.

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.

Documentación de referencia:

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

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

6.3. Estándares para los módulos criptográficos

Ver 6.2

6.3.1 Control multi-personal (n de entre m) de la clave privada

Se requiere un control multi-persona 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**

6.3.2 Custodia de la clave privada

Camerfirma no almacena ni copia claves privadas de los Firmantes cuando estas son generadas por el prestador. Para certificados en soporte hardware es el usuario quien genera y custodia la clave privada en la tarjeta criptográfica entregada por el prestador.

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

Camerfirma almacena las claves de usuario en formato PKCS#12 con objeto de reenviaras en caso de problemas en su descarga e instalación. Esta información se almacena solo por 3 días naturales. Después de este periodo se borran dichas claves.

6.3.3 Copia 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.

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.**

6.3.4 Archivo de la clave privada

Las claves privadas de las AC 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 en el proceso de generación de certificados en almacén software (PKCS#12) se asegura la eliminación de las claves de usuario ejecutando diariamente una tarea, que se elimina dichos ficheros. Esta tarea comprueba que no hayan pasado tres días hábiles desde la fecha de generación del certificado a la fecha en la que se ejecuta. La carpeta donde se almacenan los archivos tiene un filtro que impide que se realice copia de seguridad de los archivos con extensión p12.

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

6.3.5 Introducción de la clave privada en el módulo criptográfico.

Las claves de las Autoridades de certificación se crean en el interior de los dispositivos criptográficos. Ver ceremonias de creación de las claves de la Autoridad de Certificación de Camerfirma.

CONF-00-2012-01/06/07/08 **ACTAS de ceremonias de creación de claves.**

Las claves en software de los Firmantes se crean en los sistemas de Camerfirma y son entregadas al Firmante final en un dispositivo software PKCS#12. Ver procedimiento de creación de claves por el Firmante.

Las claves en hardware de los Firmantes se crean dentro del dispositivo criptográfico entregado por la AC. Ver procedimiento de creación de claves por el Firmante.

La introducción de la clave en modulo criptográfico se realizará al menos con la participación de dos personas.

Las claves asociadas a los Firmantes no pueden ser trasferidas.

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

6.3.6 Método de activación de la clave privada.

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

La clave de la AC Root se activa por un proceso de m de n. Ver apartado 6.3.1

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

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.

6.3.7 Método de desactivación de la clave privada

Para los certificados en tarjeta, la clave privada del Firmante 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, AC subordinada, TSU, se realizará una ceremonia criptográfica de la que se elaborará el acta correspondiente.

6.3.8 Método de destrucción de la clave privada

Anteriormente 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.

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

6.4. Otros aspectos de la gestión del par de claves

6.4.1 Archivo de la clave pública

La AC, 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 Firmantes y los certificados de clave pública propios.

6.4.2 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.

6.5. Datos de activación de las claves privadas.

6.5.1 Generación.

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 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 Camerfirma. Las tarjetas utilizadas por Camerfirma se generan 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 de tercero. AC Camerfirma homologa dispositivos de terceros, aunque estas disponen de una gestión independiente.

6.5.2 Protección de los datos de activación

Los datos de activación son comunicados al sujeto por un canal independiente. AC Camerfirma almacena dicha información custodia en su base de datos. 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.

6.5.3 Otros aspectos de los datos de activación

No estipulados.

6.6. Ciclo de vida del dispositivo cualificado de creación de firma.

Los certificados se almacenan las claves de Firmante en un dispositivo cualificado de creación de firma **(Hardware)**.

El dispositivo **hardware** es una tarjeta criptográfica o token USB certificado como dispositivo cualificado de creación de firma cumpliendo el anexo II de e-IDAS**.**

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.

6.7. Controles de seguridad informática

Camerfirma emplea sistemas fiables para ofrecer sus servicios de certificación. Camerfirma ha realizado controles y auditorías 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 registros de auditoría.
6. Plan de copia de respaldo y recuperación.
7. Configuración antivirus
8. Requerimientos de trafico de red

6.7.1 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 Firmante y la AC y datos de auditoria
- ✓ auditoria de eventos relativos a la seguridad
- ✓ auto-diagnóstico de seguridad relacionado con los servicios de la AC
- ✓ Mecanismos de recuperación de claves y del sistema de AC

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

9. Requerimientos de trafico de red

6.7.2 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 Firmante y la AC y datos de auditoria
- ✓ auditoria de eventos relativos a la seguridad
- ✓ auto-diagnóstico de seguridad relacionado con los servicios de la AC
- ✓ Mecanismos de recuperación de claves y del sistema de AC

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.7.3 Valoración de la seguridad informática

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

6.8. Controles de seguridad del ciclo de vida

6.8.1 Controles de desarrollo del sistema

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 realizan 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

6.8.2 Controles de gestión de la seguridad

6.8.2.1 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.

6.8.2.2 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**

6.8.2.3 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.

Camerfirma dispone de un procedimiento de bastionado de sistemas donde se define los procesos de instalación segura de equipos. Entre las medidas descritas se encuentra deshabilitar de los servicios y accesos no usados por los servicios instalados

Documentación de referencia:

CONF-2006-01-04-Procedimiento de Registro de Entradas y Salidas de Soportes
IN-2012-04-03-Procedimientos Operativos de Seguridad para el Bastionado de Sistemas.

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**

6.8.2.4 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 registro de auditoria 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.

6.8.2.5 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.

6.8.3 Evaluación de la seguridad del ciclo de vida

No estipulado

6.9. Controles de seguridad de la red

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

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

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.**

6.10. 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**

6.11. Controles de ingeniería de los módulos criptográficos

Todas las operaciones criptográficas de la AC son realizadas en módulos validados al menos por **FIPS 140-2 nivel 3**.

7. Perfiles de Certificado y CRL

7.1. Perfil de Certificado

Los perfiles de certificados cumplen el RFC 5280.

Todos los certificados cualificados o reconocidos emitidos bajo esta política están en conformidad con el estándar X.509 versión 3 y al RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.

Las fichas de 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 al correo gestion_soporte@camerfirma.com 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

- 1.2.840.113549.1.1.11 - 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 al correo gestion_soporte@camerfirma.com 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 tienen un identificador de política que parte de la base 1.3.6.1.4.1.17326.

7.1.1 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.

7.1.2 Sintaxis y semántica de los calificadores de política

No estipulado

7.1.3 Tratamiento semántico para la extensión crítica "*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 al correo gestion_soporte@camerfirma.com 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 al correo gestion_soporte@camerfirma.com 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. Especificación de la administración.

8.1. Autoridad de las políticas

El área jurídica de Camerfirma se constituye la autoridad de las políticas (PA) y es responsable de la administración de las Políticas y CPS

8.2. Procedimientos de especificación de cambios.

Esta CPS se modificará cuando se produzcan cambios relevantes en la gestión de cualquier tipo de certificados sujetos a ella. Se producirán al menos revisiones **anuales** en caso de que no se produzcan cambios en este tiempo. Estas revisiones quedaran reflejadas en el cuadro de versiones al inicio del documento.

8.2.1 Elementos que pueden cambiar sin necesidad de notificación

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 deberán con objeto de que puedan presentar sus comentarios a la organización de la administración de las políticas dentro de los **15 días siguientes a la publicación**.

8.2.2 Cambios con notificación

8.2.2.1 Lista de elementos

Cualquier elemento de esta CPS puede ser cambiado sin preaviso.

8.2.2.2 Mecanismo de notificación

Todos los cambios propuestos de esta política serán inmediatamente publicados en la Web del Camerfirma

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

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 expresamente a aquellos organismos y empresas terceras que emiten certificados bajo esta CPS.

8.2.2.3 Periodo de comentarios

Los Sujetos/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

8.2.2.4 Mecanismo de tratamiento de los comentarios

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

8.3. Publicación y copia de la política

Una copia de esta CPS estará disponible en formato electrónico en la dirección de Internet:

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

8.4. 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.

9. Anexo I. 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-Shimar-Adleman. Tipo de algoritmo de cifrado

SHA *Secure Hash Algorithm.* Algoritmo seguro de Hash

SSL *Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

TCP/IP *Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

10. Anexo II. Definiciones

Autoridad de Certificación	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza entre el 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's
CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.

Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DSADCF	*Dispositivo seguro de almacén de los datos de creación de firma.* Elemento software o hardware empleado para custodiar la clave privada del 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