DECLARACIÓN
DE
PRÁCTICAS
DE
CERTIFICACIÓN
CERTIFICADOS DIGITALES
AC CAMERFIRMA SA

Versión 3.2.3

Idioma: **Castellano**
Fecha: Diciembre 2004

Octubre 2004	v2.0	Nuevas Jerarquías. Incorporación de la política de firma de código. Corrección de erratas v2.0
Mar 2004	V2.2	Incorporación de los certificados de apoderado, sello electrónico de empresa y TSA
Junio 2006	V3	Modificación para ajustar el documento a las últimas modificaciones y a la ISO17799. Este documento servirá como documento de seguridad de LOPD y como documento de Seguridad.
Mayo 2007	V3.1	Extinción de certificados Con Poderes y Sin Poderes
Diciembre 2007	V3.1.1	Revisión de las políticas. (Modificación key usage para incorporar no repudio en los certificados de firma.
Mayo 2008	V3.1.2	Aclaraciones en el proceso de validación de certificados de sello electrónico de empresa y firma de código. Ajustes en los tipos de certificados de la jerarquía RACER con su política de certificación.
Julio 2008	V3.1.3	Incorporación de la AC Corporate Server EV. Ajustes pedidos por el auditor E&Y para auditoria WEBTRUST
Julio 2008	V3.1.4	Incorporación del apartado normativa legal aplicable. Ajustes pedidos por el auditor E&Y para auditoria WEBTRUST
Junio 2009	V3.2	Revisión completa de la redacción, incorporación certificados EV. Incorporación OID RACER. Información de las nuevas claves de ROOT 2008. Certificado de funcionario según desarrollo ley 11/2007 LAECSP. Comentarios validación titular en sello electrónico de empresa. Firma de certificados OCSP por AC. Verificación mensual de los certificados EV.
Febrero 2010	V3.2.1	Incorporación de la nueva CA intermedia de AAPP (punto 1.2.1.1 punto 5) Mejora en la descripción del proceso de emisión de certificados EV, exigido por Mozilla. Revisión general. Modificación de la descripción del responsable del certificado (punto 1.4.8 y 2.1.3). Correcciones sobre la emisión de CRL (punto 2.6.2) Correcciones alta AC AAPP (punto 6.1.1) Añadir referencia relativa al HSM ncipher (punto 6.1.8 y 6.2) Modificación 4.8. Modificación en 8.2.1
Febrero 2011	V3.2.2	Revisión E&Y proceso de auditoria renovación WebTrust
Marzo 2011	V3.2.3	Mejora en la descripción de la definición de la responsabilidad de las distintas partes del sistema de certificación, especialmente, de Camerfirma y de las AR. 2.2. 2.5.5 Política de reintegro 3.1.8 Incorporación de la autorización en los certificados de sello y firma de código. 4.5.4 Eliminación de la revocación por SMS, ya que no se usa. 5.2.2 Validación doble de las peticiones de EV. Modificación de los enlaces a la información en la página web de Camerfirma.

Índice de Contenido

1. Introducción

1.1. Consideración Inicial

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

Política de Certificación (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 Practicas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Estos conceptos de Políticas de Certificación y Declaración de Practicas de Certificación son distintos, pero aún 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 Practicas de Certificación nos dice "**cómo**" se cumplen los requerimientos de seguridad impuestos por la Política.

1.2. Vista General

El presente documento especifica la Declaración de Prácticas de Certificación de AC Camerfirma SA (en adelante, Camerfirma) para la emisión de certificados, y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de IETF, RFC 3039 del IETF y ETSI TS 101 456 V1.2.1. y en las propias políticas de certificación, siguiendo su misma estructura. Se han tenido también en cuenta las recomendaciones del documento técnico *Security Requirements for Trustworthy*

Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

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

1.2.1 Jerarquías

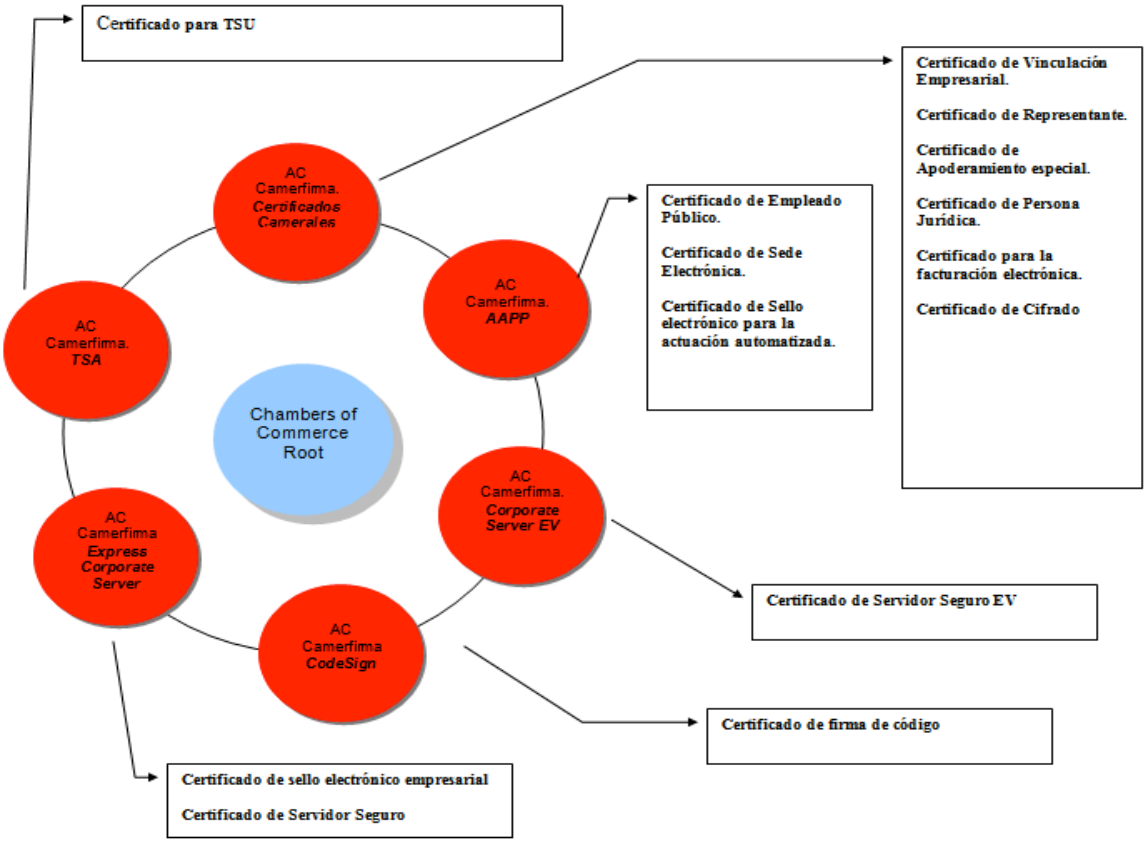
En este apartado presentaremos las jerarquías y Autoridades de Certificación (en adelante AC o AC´s) que gestiona Camerfirma. La utilización de jerarquías permite reducir los riesgos asociados a la emisión de certificados y organizarlos en diferentes AC's. Camerfirma emite dos estructuras jerarquizadas **(Chambers of Commerce Root JCC y Global Chambersign Root JCS).**

1.2.1.1 Jerarquia Chambers of Commerce Root (JCC) 1.3.6.1.4.1.17326.10.3.1

Esta Jerarquía está diseñada para construir una red de confianza que tiene por objeto fundamental la emisión de certificados digitales de identidad empresarial y donde las Autoridades de Registro (en adelante AR o AR´s) suelen encontrarse gestionadas por las Cámaras de Comercio, Industria y Navegación.

Esta jerarquía incorpora Autoridades de Certificación intermedias que emiten certificados digitales empresariales en diferentes entornos, y que son las siguientes:

- AC Express Corporate Server. 1.3.6.1.4.1.17326.10.11.1
  - Certificados para servidor Seguro 1.3.6.1.4.1.17326.10.11.2
  - Certificado de sello electrónico de empresa. 1.3.6.1.4.1.17326.10.11.3
- AC Firma de Código. 1.3.6.1.4.1.17326.10.12.1
- AC Sellos de tiempo (TSA). 1.3.6.1.4.1.17326.10.13.1
- AC Corporate Server EV. 1.3.6.1.4.1.17326.10.14.1
- AC Camerfirma Certificados Cameráles 1.3.6.1.4.1.17326.10.9.1
  - Pertenencia a Entidad. 1.3.6.1.4.1.17326.10.9.2
  - Representación. 1.3.6.1.4.1.17326.10.9.3
  - Apoderamiento Especial. 1.3.6.1.4.1.17326.10.9.5
  - Personas Jurídicas. 1.3.6.1.4.1.17326.10.9.4
  - De Factura electrónica. 1.3.6.1.4.1.17326.10.9.7
  - De cifrado. 1.3.6.1.4.1.17326.10.9.6
  - De Respondedor OCSP 1.3.6.1.4.1.17326.10.9.8
- AC Camerfirma AAPP 1.3.6.1.4.1.17326.1.3.1
  - Sede electrónica administrativa nivel alto. 1.3.6.1.4.1.17326.1.3.2.1
  - Sede electrónica administrativa nivel medio. 1.3.6.1.4.1.17326.1.3.2.2
  - Sello Electrónico para la Actuación Automatizada, nivel alto. 1.3.6.1.4.1.17326.1.3.3.1
  - Sello Electrónico para la Actuación Automatizada, nivel medio. 1.3.6.1.4.1.17326.1.3.3.2
  - Empleado Público, nivel alto, firma. 1.3.6.1.4.1.17326.1.3.4.1
  - Empleado Público, nivel alto, autenticación. 1.3.6.1.4.1.17326.1.3.4.2
  - Empleado Público, nivel alto, cifrado. 1.3.6.1.4.1.17326.1.3.4.3
  - Empleado Público, nivel medio. 1.3.6.1.4.1.17326.1.3.4.4



1.-Express Corporate Server.
De la Entidad Raíz (JCC) depende una AC intermedia llamada "**Express Corporate Server"** que emite dos tipos de certificados a maquinas o aplicativos:

- **Certificados para servidor seguro OV (Organization Validation)** mediante protocolo HTTP, necesarios para la identificación y el establecimiento de canales seguros entre el navegador del usuario o tercero que confía y el servidor de páginas HTML del Firmante/Suscriptor.
- **Certificado de sello electrónico de empresa**. Este certificado está asociado a una clave custodiada por una máquina que realiza firmas electrónicas desasistidas necesarias para dotar de integridad y autenticidad a los documentos y transacciones sobre los que se aplica. También se puede utilizar como elemento de identificación de maquina en protocolos de comunicación seguros como SSL.

2.-Firma de Código.
De la Entidad Raíz (JCC) depende una AC intermedia llamada **"Camerfirma CodeSign"** que emite certificados para la firma de código. Los certificados de código se asocian a las firmas realizadas sobre código desarrollado por

programadores (ActiveX, applets java,..etc.) estableciendo de esta forma, en dicho código, garantías de integridad y autenticidad.

3.- Sellos de tiempo.
La tercera Autoridad intermedia perteneciente a la jerarquía (JCC) está destinada a emitir certificados usados en la **emisión de sellos de tiempo**. Un sello de tiempo es un documento estandarizado que asocia el código resumen o código HASH de un documento o transacción electrónica a una fecha concreta.

La autoridad de sellado de tiempo emite certificados a entidades intermedias llamadas "Unidades de Sellado de Tiempo". Estas unidades de sellado son las que realmente emiten finalmente los sellos de tiempo, estando cada una de ellas asociadas bien a diferentes características técnicas del servicio bien al uso exclusivo de un cliente.

4.- Corporate Server EV.
Esta autoridad de certificación intermedia emite certificados digitales para Servidor Seguro o sello electrónico empresarial con la misma funcionalidad que lo hace la autoridad de certificación "Express Corporate Server" pero sujetas a los requerimientos del *"CA/Browser Forum Gidelines for Issuance and Management of extended validation certificates"*. Esta normativa impulsa la emisión de certificados de servidor seguro con garantías adicionales en el proceso de identificación de los titulares de los certificados. En este caso el nombre de la autoridad de certificación pierde su calificativo de Express ya que las garantías de acreditación para obtener el certificado son más exigentes y por lo tanto necesitan de un procedimiento más elaborado resultando un mayor plazo en su proceso de emisión.

Un certificado de Servidor Seguro 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

5.- AC Camerfirma Certificados Camerales.
La siguiente y última entidad intermedia de la jerarquía pertenece a **Camerfirma;** esta entidad emite certificados de vinculación empresarial para el territorio español. "AC Camerfirma Certificados Camerales" es una Autoridad de Certificación multipolítica que emite en su mayor parte certificados cualificados o reconocidos conformes los criterios establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica cuyas funcionalidades se describen a continuación.

También de forma puntual emite certificados de forma exclusiva para el respondedor de verificación del estado de certificado OCSP de Camerfirma. Las respuestas del servicio OCSP de Camerfirma van firmadas electrónicamente con un certificado de este tipo.

Los certificados finales se dirigen a:

Personas físicas con atributo de vinculación a Entidad.

- ✓ **Pertenencia a Entidad .**
  Determinan la relación de vinculación (laboral, mercantil, colegial, etc.) entre una persona física (titular del certificado/firmante/suscriptor) y una Entidad (campo organización del certificado).
- ✓ **Representación.**
  Determina la relación de representación legal o de apoderado general entre la persona física (titular del certificado/firmante/suscriptor) y una Entidad (descrita también en el campo Organización del certificado).
- ✓ **Apoderamiento Especial**.
  Determina la relación de representación específica ó de apoderamiento especial entre una persona física (titular del certificado/firmante/suscriptor) y una Entidad (descrita también en el campo Organización del certificado).

Personas Jurídicas.

El certificado digital de Persona Jurídica se crea a partir de la **Ley 59/2003** de Firma Electrónica, de 19 de diciembre.

Camerfirma emite estos certificados para aquellos actos que integren la relación entre la Entidad (Persona Jurídica) y las Administraciones públicas (relaciones tributarias, emisión de factura electrónica…) y, en general, tal y como determina la legislación vigente para aquellos tramites que constituyen el giro o tráfico ordinario de la Entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse.

"Camerfirma emite estos certificados principalmente para su uso en el ámbito tributario permitiendo a las empresas la realización de trámites telemáticos con la Agencia Estatal de la Administración Tributaria. Fuera de este ámbito Camerfirma considera estos certificados similares al sello de empresa y el Tercero que confía deberá valorar el uso de la firma asociada a este tipo de certificado como tal.". Un sello dota al documento asociado de las garantías técnicas de Autenticidad y de integridad."

En el caso del certificado de Persona Jurídica, el titular/suscriptor/firmante es la propia Entidad, aunque únicamente puede ser solicitado por un representante legal ó voluntario de la Entidad con poder suficiente a estos efectos, que actuará como custodio de las claves y persona responsable de las actuaciones que se realicen con dicho certificado, aunque se contempla la posibilidad de ceder las claves a una tercera persona o de incorporarlas a un

aplicativo informático para responder a las necesidades de las practicas habituales de cada usuario.

De Factura electrónica.

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

De cifrado.

El certificado de cifrado es un certificado técnico que permite el uso exclusivo de cifrado de datos. Los certificados de persona física de pertenencia a entidad, de representante, de apoderamiento especial, de facturación electrónica y de persona jurídica anteriormente descritos permiten el uso de la clave para el cifrado de datos pero Camerfirma no custodia ni almacena las claves privadas de los titulares de los certificados cumpliendo así los requerimientos de la **Ley 59/2003** de Firma Electrónica, de 19 de diciembre. En esta situación si el titular del certificado ó, en el caso del certificado de persona jurídica, el custodio del certificado, perdiera el control sobre la clave privada, perdería también el acceso a todos los datos cifrados con la clave pública asociada. El certificado de cifrado permite al prestador de los servicios, es decir en este caso a Camerfirma, custodiar la clave privada del titular del certificado para reponerla en caso de pérdida.

De Respondedor OCSP

Este certificado se emite únicamente al respondedor de estado de certificados emitidos por AC Camerfirma Certificados Camerales y sirve para validar las respuestas del servicio de validación en línea.
Cada Autoridad de Certificación emitirá un certificado bajo esta política con el fin de que el respondedor OCSP firme las respuestas de forma autorizada.

6.- AC Camerfirma AAPP.

Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) establece en el Capítulo Segundo, Título Segundo, los mecanismos de aplicación por las Administraciones Públicas (AAPP) para la identificación y firma electrónica basada en certificados electrónicos.

Dentro de la LAECSP se 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.

AC Camerfirma en base a lo anterior y bajo el esquema de identificación y firma de la AGE y específicamente su política de certificación, emitirá los siguientes tipos de certificados:

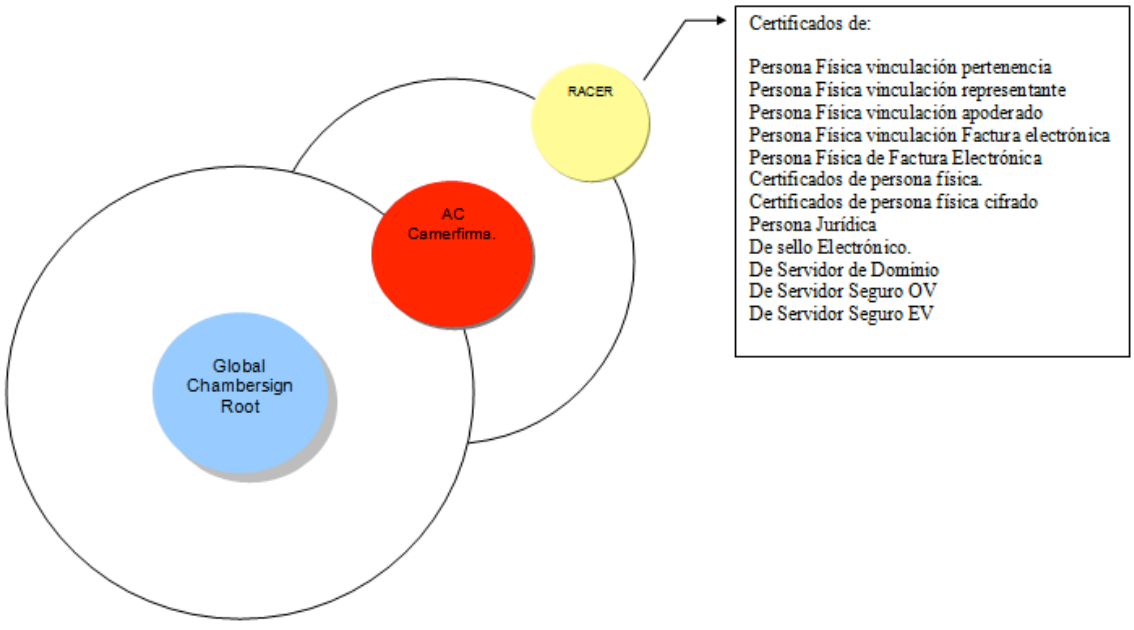
- Certificado reconocido de Sello Electrónico para la Actuación Automatizada, nivel alto.
- Certificado reconocido de Sello Electrónico para la Actuación Automatizada, nivel medio.
- Certificado reconocido de de Empleado Público, nivel alto, firma.
- Certificado reconocido de de Empleado Público, nivel alto, autenticación.
- Certificado reconocido de de Empleado Público, nivel alto, cifrado.
- Certificado reconocido de Empleado Público, nivel medio.
- Certificado sede electrónica administrativa nivel medio.
- Certificado sede electrónica administrativa nivel alto.

1.2.1.2 Jerarquía Chambersign Global ROOT (JCS) 1.3.6.1.4.1.17326.10.1.1

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 del proyecto. En este sentido, y a diferencia de la JCC, las Autoridades de Registro no tienen porque encontrarse enmarcadas en el ámbito de las Cámaras de Comercio, ni donde los certificados emitidos tienen porque encontrarse enmarcado en un ámbito empresarial ó de vinculación a entidad.

También en el marco de esta Jerarquía penden distintas Autoridades de Certificación intermedias:

- AC Camerfirma 1.3.6.1.4.1.17326.10.4.1
  - RACER 1.3.6.1.4.1.17326.10.8.1
    - Certificado de Persona Física de Vinculación Pertenencia 1.3.6.1.4.1.17326.10.8.2
    - Certificado de Persona Física de Vinculación Representación 1.3.6.1.4.1.17326.10.8.3
    - Certificado de persona jurídica 1.3.6.1.4.1.17326.10.8.4
    - Certificado de Sello Electrónico 1.3.6.1.4.1.17326.10.8.5
    - Certificado de Persona Física 1.3.6.1.4.1.17326.10.8.6
    - Certificado de Persona Física de Vinculación Factura Electr. 1.3.6.1.4.1.17326.10.8.7
    - Certificado de Persona Física de Vinculación Apoderado 1.3.6.1.4.1.17326.10.8.8
    - Certificado de Persona Física de cifrado 1.3.6.1.4.1.17326.10.8.9



1.- AC Camerfirma

El objeto de esta AC intermedia será la de emitir certificados sectoriales, y de la que pende a su vez la siguiente Autoridad de Certificación de segundo nivel RACER

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

Aunque **RACER** es una AC multipolítica de propósito general que emite certificados de entidad final, lo cierto es que la mayor parte de los certificados emitidos bajo esta AC, en el marco de proyectos concretos, tienen un carácter de vinculación a entidad, y así se suelen emitir:

- Certificado de pertenencia a entidad
- Certificado de representante
- Certificado de apoderamiento
- Certificado de facturación electrónica
- Certificado de persona jurídica
- Certificado de sello electrónico.

Aunque como AC RACER tiene este carácter abierto, los anteriores certificados pueden tener una estructura distinta a la definida bajo JCC: También bajo esta AC se vienen pudiendo solicitar certificados de persona física que **no determinan** la relación ó vinculación de la persona física con una entidad jurídica y simplemente garantiza la identidad de la persona física como Firmante/ Suscriptor, titular del certificado.

1.2.2 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 es el departamento jurídico de Camerfirma. El departamento jurídico de Camerfirma 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.

Puede contactar con la Autoridad de las Políticas (PA) en:

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 se informe a este respecto. En la Web de Camerfirma se puede encontrar información general sobre el uso de la firma digital y los certificados digitales.

1.3. Identificación

Nombre:	CPS Camerfirma SA
Descripción:	Documento de respuesta a los requerimientos de las Políticas con identificativo: 1.3.6.1.4.1.17326.10.8.x 1.3.6.1.4.1.17326.10.9.x 1.3.6.1.4.1.17326.10.10.x 1.3.6.1.4.1.17326.10.11.x 1.3.6.1.4.1.17326.10.12.x 1.3.6.1.4.1.17326.10.13.x 1.3.6.1.4.1.17326.10.14.x 1.3.6.1.4.1.14862.1.3 Política general de certificación de la Administración General del Estado.
Versión:	3.2.1
Fecha primera Emisión:	Noviembre 2008
Localización:	http://www.camerfirma.com

1.4. Comunidad y Ámbito de Aplicación.

1.4.1 Autoridad de Certificación (AC).

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

A los efectos de la presente CPS todas las Autoridades de Certificación son gestionadas por Camerfirma.

La información relativa a la AC puede encontrarse en la dirección Web http://www.camerfirma.com

1.4.2 Entidad de Acreditación

La entidad de acreditación será el órgano gestor correspondiente que admite, acredita y supervisa las entidades de certificación. Esta tarea recae en el Ministerio de Industria Turismo y Comercio.

1.4.3 Prestador de servicios de certificación (PSC).

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

A los efectos de la presente CPS, Camerfirma es el PSC.

1.4.4 Autoridad de Registro (AR)

Ente que actúa conforme esta CPS y, en su caso, mediante acuerdo suscrito con una AC concreta, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y aquellas que se dispongan en las Políticas de Certificación concretas. Las AR son autoridades delegadas de la AC aunque ésta, es la última responsable del servicio. La AC puede en cualquier momento ejercer las labores de AR.

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

Para la Jerarquía Chambers of Commerce Root (JCC):

- La propia Autoridad de Certificación.
- Las Cámaras de Comercio, Industria y Navegación ó aquellas entidades delegadas por éstas. El proceso de registro puede ser realizado por parte de diferentes entidades delegadas mediante:
  - Puntos de verificación presencial (PVP): Entidades que realizan la verificación presencial del titular del certificado. No tienen capacidad de registro pero se vinculan contractualmente con una AR para que ésta última, en base a la documentación recogida por el PVP, realice el registro y la petición del certificado a la AC.
  - AR Empresarial: Es una entidad delegada por la AR para llevar los registros de una pluralidad de Firmantes/Suscriptores pertenecientes a una misma organización o entidad concreta dentro de la jurisdicción de una AR, pudiendo ser por ejemplo: los empleados de una corporación, los asociados de una agrupación empresarial, los colegiados de un colegio profesional. Los operadores de dichas AR empresariales solo podrán gestionar las solicitudes y los certificados en el ámbito de dicha organización.
- La Administración Pública, en el caso de los certificados emitidos bajo la AC Camerfirma AAPP.

Para la Jerarquía Chambersign (JCS).

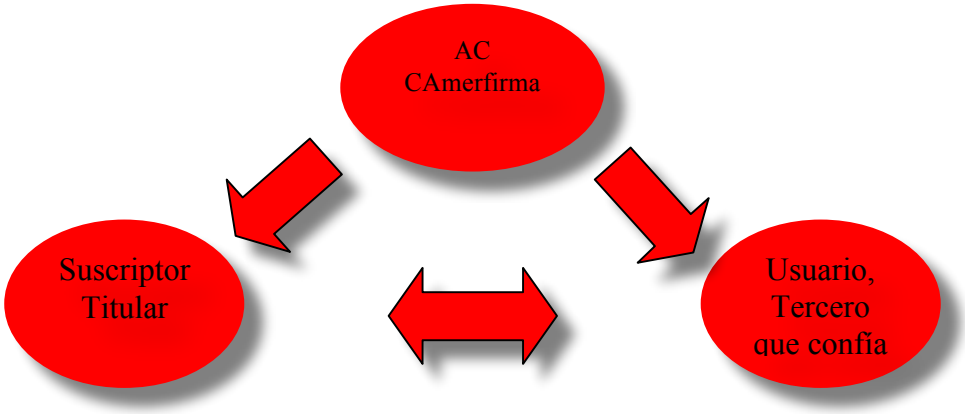
- La propia Autoridad de Certificación.
- Cualquier agente nacional o internacional que mantenga una relación contractual con la AC, supere los procesos de alta y las Auditorias exigidas en las Políticas de Certificación**.**

1.4.5 Firmante/ Suscriptor.

Entendemos por Firmante/Suscriptor, al Titular del certificado cuando éste sea una persona física o jurídica. Cuando se emita a nombre de un dispositivo hardware o aplicativo informático, se considerará firmante/Suscriptor, la persona jurídica asociada al certificado emitido.

1.4.6 Tercero que confía o usuario del certificado.

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



1.4.7 Entidad.

En los certificados digitales de persona física con atributo empresarial, la Entidad se constituye como aquella empresa u organización con la que el Firmante/Suscriptor mantiene una vinculación determinada que aparece definida en el campo atributo de cada certificado.
Y así

- ✓ En el caso del certificado de Persona física de vinculación, la Entidad se encuentra vinculada al Firmante/Suscriptor mediante una relación mercantil, laboral, colegial, etc.

- ✓ En el caso del certificado de Representante, la Entidad se encuentra representada con amplios poderes por el Firmante/Suscriptor.

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

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

- ✓ En el caso de certificados de Servidor Seguro/Sello electrónico de Empresa, la Entidad es la titular del dominio de Internet o del aplicativo para el cual se ha pedido el certificado.

Como norma general la Entidad queda identificada dentro del certificado en el campo organización y su identificador fiscal en el campo numero de serie. Para mas información ver el apartado 3.1.1.

La única excepción a lo anteriormente expuesto, es en aquellos casos donde la Entidad coincide con la figura del Firmante/ Suscriptor (certificado de persona jurídica).

1.4.8 Solicitante.

Se entenderá por Solicitante la persona física que solicita el Certificado al PSC Camerfirma, pudiendo ser el propio Firmante/Suscriptor ó una persona autorizada por el mismo.

1.4.9 Responsable de certificados

El responsable es la persona física encargada de la custodia de los datos de las claves criptográficas asociadas al certificado.

Bajo esta CPS, el responsable de los certificados suele coincidir con la figura del Solicitante.

El responsable de las claves suele estar descrito dentro del contenido del certificado en los atributos: Apellidos y Nombre del campo Titular.

1.4.10 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.

1.4.10.1 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.

El empleo de los certificados digitales en operaciones que contravienen las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS o los Contratos de la AC con

las AR ó con sus Firmantes/Suscriptores tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

Camerfirma no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de Camerfirma emitir valoración alguna sobre dicho contenido, asumiendo por tanto el 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 sus Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

Camerfirma incorpora en el certificado información sobre la limitación de uso bien, en campos estandarizados en los atributos "uso de la clave" "key usage" y "restricciones básicas" "Basic Constrains" marcados como críticos en el certificado y por lo tanto de cumplimiento obligatorio por parte de las aplicaciones que lo utilicen, o bien mediante textos incorporados el campo "user notice" de uso "no critico" pero de obligado cumplimiento por parte del titular y del usuario del certificado.

1.5. Normativa legal aplicable

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

1.6. 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 C/ Ribera del Loira, 122 8042 MADRID Teléfonos: 902 361 207 +34 914 119 661 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 esta CPS y en las Políticas de Certificación.
- ✓ Proteger sus claves privadas de forma segura.
- ✓ Emitir certificados conforme a esta CPS, a las Políticas de Certificación y a los estándares 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 Firmantes/Suscriptores 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 Firmantes/Suscriptores y a las AR's que estén vinculadas a ella.
- ✓ No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor.
- ✓ 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 AR

Las AR son las entidades delegadas por Camerfirma para realizar esta labor, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

- ✓ Respetar lo dispuesto en esta CPS y en la Política de Certificación correspondiente.
- ✓ Proteger sus claves privadas.

- ✓ Comprobar la identidad de los Firmantes/Suscriptores y Solicitantes de los certificados.
- ✓ Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- ✓ Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o suscriptor.
- ✓ Respetar lo dispuesto en los contratos firmados con Camerfirma y con el Firmante/Suscriptor
- ✓ Informar a Camerfirma de las causas de revocación, siempre y cuando tomen conocimiento.
- ✓ Asumir dichas obligaciones incluso en los casos de entidades delegadas por éstas (a PVP o AR Empresarial)

2.1.2 Solicitante/Responsable del certificado.

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

- ✓ Suministrar a la AR la información necesaria para realizar una correcta identificación.
- ✓ Garantizar la exactitud y veracidad de la información suministrada.
- ✓ Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- ✓ Custodiar su clave privada de manera diligente.

2.1.3 Firmante/Suscriptor.

El Firmante/Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- ✓ Usar el certificado según lo establecido en la presente CPS y en las Políticas de Certificación aplicables.
- ✓ Respetar lo dispuesto en los documentos firmados con Camerfirma y la AR.
- ✓ Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión /revocación.
- ✓ Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- ✓ No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por Camerfirma o la AR de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.

2.1.4 Tercero que confía/Usuario.

Será obligación del Tercero que confía cumplir con lo dispuesto por lo dispuesto en la normativa vigente y además:

- Verificar la validez de los certificados antes de realizar cualquier operación basada en los mismos. Camerfirma dispone de diversos mecanismos para realizar dicha comprobación como el acceso a listas de revocados o a servicios de consulta en línea como OCSP, todos estos mecanismos están descritos en la página Web de Camerfirma http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

2.1.5 Entidad

En el caso de aquellos certificados que impliquen vinculación a una Entidad, la Entidad vendrá obligada a solicitar a la AR la suspensión/revocación del certificado cuando el Firmante/Suscriptor cese dicha vinculación respecto a la organización.

2.1.6 Repositorio

Camerfirma dispone de un servicio de consulta de certificados emitidos y listas de revocación. Estos servicios están disponibles públicamente en su página Web http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

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

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

2.2. Responsabilidad.

La responsabilidad de Camerfirma

El artículo 22.1 de la Ley de Firma Electrónica establece que: "*Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que impone esta Ley.*

La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible."
Así pues Camerfirma será responsable de los daños y perjuicios ocasionados a los usuarios por sus servicios, ya sea al Firmante/Suscriptor ó al Tercero que confía, y a otros terceros en los términos establecidos en la legislación vigente y en las Políticas de Certificación.

En este sentido Camerfirma es la única responsable (i) de la emisión de los certificados, (ii) de su gestión durante todo el ciclo de vida de éstos y (iii) en particular, si es preciso, en caso de suspensión y revocación de los certificados. En concreto, Camerfirma fundamentalmente será responsable de:

La exactitud de toda la información contenida en el certificado en la fecha de su emisión, mediante la confirmación de los datos del solicitante y las prácticas de AR.

La garantía de que, en el momento de la entrega del certificado, obra en poder del Firmante/Suscriptor, la clave privada correspondiente a la clave pública dada o identificada en el certificado cuando el proceso así lo requiera, mediante la utilización de peticiones estandarizadas en formato PKCS#10.

La garantía de que la clave pública y privada funcionan conjunta y complementariamente, utilizando dispositivos y mecanismos criptográficos certificados.

La correspondencia entre el certificado solicitado y el certificado entregado.

Cualquier responsabilidad que se establezca por la legislación vigente.

En cumplimiento de la legislación vigente Camerfirma dispone de un seguro de responsabilidad civil que cubre los requerimientos marcados por las políticas de certificación afectadas por éstas prácticas de certificación.

La responsabilidad de las AR

Las AR han suscrito un contrato de prestación de servicio con Camerfirma mediante el cual Camerfirma delega las funciones de registro en las AR, 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 ó 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.
- 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 AR se responsabilizan de las consecuencias en caso de incumplimiento o cumplimiento incorrecto 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 AR y que deberán servirles de manual de referencia.

En caso de reclamación por un Firmante, una Entidad, ó Tercero que Confia, 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 AR, hacer soportar a la AR responsable la asunción de las consecuencias. Porque, aunque legalmente sea la AC la persona jurídica responsable frente al Firmante, una Entidad, ó Tercero que Confia, y que para ello dispone de un seguro de responsabilidad civil, según el acuerdo vigente y las Políticas y PC's vinculantes, la AR 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 AR en cuanto a los posibles daños cuyo origen vendría de un incumplimiento de las tareas delegadas a las AR. Por esta razón, al igual que lo previsto para la AC, la AR 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 AR mediante la realización de auditorias para evaluar entre otros, los recursos empleados y el conocimiento y control de los procedimientos operativos para ofrecer los servicios de AR

2.2.1 Exoneración de responsabilidad

Según la legislación vigente, la responsabilidad de CAMERFIRMA y de la AR no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Firmante, y al Tercero que confía 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 al Tercero que confía 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 limite de importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado
- De los daños ocasionados al firmante 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 AR's tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

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

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 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 Firmante/Suscriptor y el Tercero que confía, 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 vigente.

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 cualquiera otros servicios relacionados están disponibles y actualizados en la página Web de Camerfirma http://www.camerfirma.com/camerfirmaPublic/index/certificados.html.

Cada tipo de certificado tiene publicado su precio concreto.

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.

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 gratuito a través de listas de certificados revocados o mediante acceso vía Web en la dirección Internet de Camerfirma http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

Camerfirma se reserva el derecho a facturar por servicios de validación de valor añadido como **OCSP**. Las tarifas de estos servicios estarán publicadas en la dirección http://www.camerfirma.com/camerfirmaPublic/index/Servicios/OCSP.html.

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

El acceso al contenido de la presente CPS es gratuito, en la dirección Web de Camerfirma http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html.

2.5.5 Política de reintegros.

AC Camerfirma no tiene una política de reintegros especifica, y se acoge a la normativa general vigente sobre comercio electrónico.

2.6. Publicación y repositorios.

2.6.1 Publicación de información de la AC.

2.6.1.1 Políticas y Prácticas de Certificación.

La presente CPS y Políticas actuales están disponibles públicamente en el sitio de Internet: http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html

2.6.1.2 Términos y condiciones.

Camerfirma pone a disposición de los usuarios, los términos y condiciones del servicio, en sus políticas y practicas de certificación. El firmante/Suscriptor 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.

2.6.1.3 Difusión de los certificados.

Se podrá acceder a los certificados emitidos, siempre ***que el Firmante/Suscriptor de su consentimiento***, en el sitio de Internet:
http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

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

Se podrá ofrecer esta información a través de un servicio LDAP. En el momento en que este servicio este a disposición del cliente se describirá en estas prácticas los detalles del servicio.

2.6.2 Frecuencia de publicación.

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

AC Camerfirma emite y publica **listas de revocados** de forma periódica siguiendo la siguiente tabla, e inmediatamente después de producirse una revocación.

CA	Se emiten cada..	Duración
CHAMBERS OF COMMERCE ROOT	180 días	180 días
CAMERFIRMA CERTIFICADOS CAMERALES	24 horas	48 horas
CAMERFIRMA AAPP	24 horas	48 horas
CAMERFIRMA EXPRESS CORPORATE SERVER v3	24 horas	48 horas
CAMERFIRMA CODESIGN v2	24 horas	48 horas
CAMERFIRMA TSA	30 días	30 días

CHAMBERSIGN ROOT	180 días	180 días
AC CAMERFIRMA	180 días	180 días
RACER	24 horas	48 horas

CHAMBERS OF COMMERCE ROOT -2008	365 días	365 días
CAMERFIRMA CERTIFICADOS CAMERALES - 2009	24 horas	48 horas
CAMERFIRMA AAPP- 2010	24 horas	48 horas
CAMERFIRMA CORPORATE SERVER - 2009	24 horas	48 horas
CAMERFIRMA CODESIGN - 2009	24 horas	48 horas
CAMERFIRMA TSA - 2009	30 días	30 días

CHAMBERSIGN ROOT - 2008	365 días	365 días
CAMERFIRMA	365 días	365 días
RACER	24 horas	48 horas

Camerfirma publica de forma inmediata en su página Web http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html cualquier modificación en las **Políticas y la CPS**, manteniendo un histórico de versiones.

2.6.3 Controles de acceso

Camerfirma emplea un su página Web para la publicación y distribución de certificados y CRL's. Se empleara por lo tanto un protocolo HTTP para acceder a la lista de revocación y para el acceso al directorio de certificados se necesitara el email del titular 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.

2.7. Auditorias

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 27001:2005, y la realización de Auditorias 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 auditorias periódicas con el sello **WEBTRUST for CA y WEBTRUST EV** que asegura que los documentos de políticas y CPS tienen un formato y alcance adecuado a la vez que están completamente alineadas.

Camerfirma ha pasado en el año 2007 un proceso de inspección ordinaria del Ministerio de Industria. El Ministerio de Industria es el ente regulador encargado de supervisar las actividades llevadas a cabo por los prestadores de servicios de certificación españoles.

2.7.1 Frecuencia de las auditorias

Ver 2.7

2.7.2 Identificación y calificación del auditor

Las auditorias son realizadas por la compañía externa de amplio reconocimiento.

- Para la auditoria WEBTRUST Ernst & Young. http://www.ey.com/ES/es/home.
- Para las auditorias ISO27001 AENOR. http://www.aenor.es/aenor/inicio/home/home.asp
- Para las auditorias internas Start-Up http://www.seguridadinformacion.com/

2.7.3 Relación entre el auditor y la AC

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorias informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la AC.

2.7.4 Tópicos cubiertos por la auditoria

La auditoria verifica:

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 sus sistemas de información
e) En los certificados de EV la auditoría interna realizará una muestra del 3% de los certificados emitidos para su análisis.

2.7.5 Auditoria en las Autoridades de Registro

Todas las AR son auditadas. Estas auditorías se realizan al menos cada dos años y 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.

Camerfirma realizará las auditorias a las AR.
La empresa Start-Up realiza el proceso de auditoría de la red completa de RAs cada dos años.

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

Documentación de referencia:

IN-2010-04-12-Procedimiento de Evaluación de la Seguridad en AR's
IN-2010-04-15-Ficha de la visita de evaluación.doc
IN-2010-04-16-Lista de Chequeo
IN-2006-03-08-Procedimiento Labores de AR.
IN-2010-04-17-Informe de evaluación

2.8. Confidencialidad

2.8.1 Tipo de información a mantener confidencial

Camerfirma considerará confidencial toda la información que no esté catalogada expresamente como publica. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter de confidencialidad, 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 que deberán firmar todas las personas que tengan acceso a información confidencial.

Camerfirma cumple en todo caso con la normativa vigente en materia de protección de datos. Respecto a este aspecto este documento sirve según la ley de firma 59/2003 como documento de seguridad.

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 siempre que el Firmante/Suscriptor haya otorgado su consentimiento.
c) Cualquier información cuya publicidad sea impuesta 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.

Se dispone de un servicio de consulta de CRL y Certificados en el sitio de Internet http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html, así como información de los distintos métodos de consulta del estado de los certificados digitales.

2.8.4 Envío a la Autoridad Competente

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

2.9. Derechos de propiedad intelectual

La propiedad intelectual de esta CPS pertenece a Camerfirma.

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Tipos de nombres

El Firmantes/Suscriptor se describe en los certificados mediante un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

El DN del Firmante/Suscriptor del certificado tendrá el formato siguiente:

Para Certificados de las Jerarquías JCC y JCS:

De persona física y representante.

C= País de la organización
CN = <Nombre y Apellidos del suscriptor>[ACRONIMO]
E = <mail del suscriptor>
SN = <NIF del suscriptor>
Surname = <Apellidos del suscriptor>
Given name = <Nombre del suscriptor>
1.3.6.1.4.1.17326.30.3 ES= <número de documento identificativo del suscriptor>
O = <Nombre organización>
OU = <Departamento>
T = <Cargo del suscriptor en la organización>
Description = Descripción del tipo de certificado.

De apoderado.

C= País de la organización
CN = <Nombre y Apellidos del suscriptor> [ACRONIMO]
E = <mail del suscriptor>
SN=Número de documento identificativo de la organización
Surname = <Apellidos del suscriptor>
Given name = <Nombre del suscriptor>
1.3.6.1.4.1.17326.30.3 ES= <número de documento identificativo del suscriptor>
O = <Nombre organización>
OU = <Departamento>
T = <Cargo del suscriptor en la organización>
T = <Poderes del suscriptor>
Description = Descripción del tipo de certificado.

De persona Jurídica.

C= País de la organización
CN = <Razón social del solicitante>
E = <mail del representante>
SN=Número de documento identificativo de la organización
Surname = <Apellidos del representante>
Given name = <Nombre del representante>
1.3.6.1.4.1.18838.1.1 (AEAT) = <NIF del representante>
O = <Nombre de la organización>
OU = <Departamento del representante>
T = <Cargo del representante>
Description = Descripción del tipo de certificado.

De servidor.

SN=Número de documento identificativo de la organización
E = <mail del suscriptor>
CN = URL de la organización
O = <Nombre de la organización>
OU = <Departamento del suscriptor>
S=Provincia de la organización
L=Localidad de la organización
C= País de la organización

De servidor EV.

C= País de la organización
CN= URL de la organización
S=Provincia de la organización
L=Localidad de la organización
PostalCode= Código postal de la organización
Street= Dirección de la organización
O=Nombre de la organización
OU=Departamento dentro de la organización
SN=Número de documento identificativo de la organización
2.5.4.15= Categoría de la organización (privada, gobierno, negocio)
1.3.6.1.4.1.311.60.2.1.3 = País del registro
1.3.6.1.4.1.311.60.2.1.2 = Provincia del registro
1.6.13 1.3.6.1.4.1.311.60.2.1.1 =Localidad del registro

De Sello electrónico.

C= País de la organización
CN= Nombre o descripción de la Aplicación
O=Nombre de la organización
OU=Departamento dentro de la organización
S=Provincia de la organización
L=Localidad de la organización
E = <mail del suscriptor>
SN=Número de documento identificativo de la organización

De firma de código.

C= País de la organización
CN = Nombre o descripción de la Aplicación
SN=Número de documento identificativo de la organización
O=Nombre de la organización
S=Provincia de la organización
L=Localidad de la organización
SN=Número de documento identificativo de la organización

De Cifrado.

Todos estos campos del DN del certificado son los mismos que en el certificado de autenticación con el que se ha obtenido con una única diferencia, en el CN aparece la cadena '(CIFRADO)'.

De factura electrónica.

C= País de la organización
CN=<Nombre del Firmante/Suscriptor [ACRONIMO] / Pseudónimo
E=<mail del titularl>
SN=<NIF del titular>
Surname=<Apellidos del titular >
Given name=<Nombre del titular >
1.3.6.1.4.1.17326.30.3=ES<número de documento identificativo>
O=<Nombre organización>
OU=<Departamento del titular>
OU="FACTURACION ELECTRONICA"
T=<Cargo del titular>

De Empleado Público.

C= País de la organización
CN = <Nombre del Firmante/Suscriptor - DNI
Given name=<Nombre del titular >
Surname=<Apellidos del titular >- DNI
SN=< DNI/NIE del empleado público.>
T=<Cargo del titular>
OU = <número de documento identificativo del Organismo>
OU=<Departamento del titular>
OU = EMPLEADO PUBLICO
O=<Nombre del Organismo>

Por la presente Declaración de Prácticas de Certificación, Camerfirma utilizará el esquema de nombres normalizado propuesto por la AGE ("Identidad Administrativa") para cada tipo y perfil de certificado emitido. De este modo se utiliza un marco común, asignando exactamente el mismo

nombre a sellos, sedes, organizaciones, puestos y unidades, etc. para toda la Administración Pública Estatal.

El objeto Identidad Administrativa utilizará el número ISO/IANA del MAP 2.16.724.1.3.5.X.X como base para identificarlo, de este modo se establecería un identificador unívoco a nivel internacional. Esta información se localiza en el campo "nombre alternativo del sujeto" del certificado.

2.16.724.1.3.5.3.1CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO (Nivel Alto)

2.16.724.1.3.5.3.2= CERTIFICADO ELECTRÓNICO DE EMPLEADO PUBLICO (Nivel Medio)

De Sello electrónico para la actuación automatizada.

C= País de la organización
CN = Nombre o descripción de la Aplicación
Given name=<Nombre del responsable de las claves>
Surname=<Apellidos del responsable de las claves >- DNI
SN=<NIF del organismo>
OU = SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA
O=<Nombre del Organismo>

Por la presente Declaración de Prácticas de Certificación, Camerfirma utilizará el esquema de nombres normalizado propuesto por la AGE ("Identidad Administrativa") para cada tipo y perfil de certificado emitido. De este modo se utiliza un marco común, asignando exactamente el mismo nombre a sellos, sedes, organizaciones, puestos y unidades, etc. para toda la Administración Pública Estatal.

El objeto Identidad Administrativa utilizará el número ISO/IANA del MAP 2.16.724.1.3.5.X.X como base para identificarlo, de este modo se establecería un identificador unívoco a nivel internacional. Esta información se localiza en el campo "nombre alternativo del sujeto" del certificado.

2.16.724.1.3.5.2.1=SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Alto)
2.16.724.1.3.5.2.2=SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA (Nivel Medio)

De Sede electrónica.

C= País de la organización
CN = Denominación de nombre de dominio (DNS o IP)
Given name=<Nombre del responsable de las claves>

Surname=<Apellidos del responsable de las claves >- DNI
SN=<NIF del organismo>
OU = SEDE ELECTRONICA
OU = El nombre descriptivo de la sede.
O=<Nombre del Organismo>

Por la presente Declaración de Prácticas de Certificación, Camerfirma utilizará el esquema de nombres normalizado propuesto por la AGE ("Identidad Administrativa") para cada tipo y perfil de certificado emitido. De este modo se utiliza un marco común, asignando exactamente el mismo nombre a sellos, sedes, organizaciones, puestos y unidades, etc. para toda la Administración Pública Estatal.

El objeto Identidad Administrativa utilizará el número ISO/IANA del MAP 2.16.724.1.3.5.X.X como base para identificarlo, de este modo se establecería un identificador unívoco a nivel internacional. Esta información se localiza en el campo "nombre alternativo del sujeto" del certificado.

2.16.724.1.3.5.1.1=SEDE ELECTRONICA (Nivel Alto)
2.16.724.1.3.5.1.2=SEDE ELECTRONICA (Nivel Medio)

Para certificados de la Jerarquía JCS

Los certificados de la jerarquía **JCS** comparten la misma descripción del campo titular, con la diferencia de que incorporan varios campos privados más en el DN indicando los tipos de documento que se ha utilizado para la acreditación de la identidad de la organización y del titular del certificado:

1.3.6.1.4.1.17326.30.2 → Tipo de documento que identifica a la organización
1.3.6.1.4.1.17326.30.4 → Tipo de documento que identifica al titular del certificado
1.3.6.1.4.1.17326.30.5 → IFE de México
1.3.6.1.4.1.17326.30.6 → RFC de México

3.1.2 Pseudónimos

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

El cálculo del seudónimo en aquellos certificados donde se permita, se realiza de manera que se identifica unívocamente al titular real del **certificado anexando al número de serie del certificado más un acrónimo de la organización.**

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

No se puede volver a asignar un nombre de suscriptor que ya haya sido ocupado, a un suscriptor diferente.

El atributo (identificador de la empresa) y el SN se usan para distinguir entre dos identidades cuando exista algún problema sobre duplicidad de nombres.

3.1.5 Procedimiento de resolución de disputas de nombres

Camerfirma no tiene responsabilidad en el caso de resolución de disputas de nombres.
La asignación de nombres se realizara basándose en su orden de entrada.

Camerfirma no arbitrara 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 las marcas registradas

Camerfirma no asume compromisos en la emisión de certificados respecto al uso de una marca comercial. Camerfirma no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Firmante/Suscriptor. Sin embargo, Camerfirma no está obligada a buscar evidencias de la posesión de marcas registradas antes de 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 la AC.

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 vienen descritos en las Políticas correspondientes. En los certificados de Servidor seguro, las claves son generadas por el usuario utilizando las

herramientas ofrecidas por el programa de servidor de páginas donde finalmente se instalara.

a) Generación de claves por parte de Camerfirma.

   Se entregan al suscriptor en mano o mediante correo mediante ficheros protegidos utilizando el Standard **PKCS#12**. La seguridad del proceso queda garantizada ya que la clave de acceso al fichero, que posibilita la instalación de este en las aplicaciones, es entregada por un medio distinto al utilizado en la entrega del P12 (correo, teléfono, entrega personal, SMS…)

   Las claves pueden ser entregadas por Camerfirma al Firmante/Suscriptor, directamente o a través de una AR, en una tarjeta criptográfica (DSCF). En este caso consideramos la entrega en dispositivo hardware.

b) Generación de las claves por el suscriptor.

   El suscriptor 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**.

   Cuando el suscriptor crea sus propias claves en un dispositivo criptográfico y pide a Camerfirma emitir un certificado digital con una política de generación de claves en dispositivo hardware, el suscriptor debe acompañar a la petición un acta de creación de claves avalado por un auditor externo independiente que evaluara el operador de la AR. Este procedimiento asegura que las claves realmente han sido generadas en un dispositivo hardware tal y como se dirá el certificado emitido.

   AC Camerfirma se reserva el derecho a valorar el aval del auditor externo como valido o bien rechazarlo.

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 AR, exige:

<u>En los Certificados reconocidos:</u>

- Identificación del Solicitante:
  Se exige la personación física del Firmante/Suscriptor cuando éste es también Solicitante o de un representante del Solicitante cuando éste es una entidad jurídica, así como la presentación de su Documento Nacional de

Identidad, tarjeta de residencia o pasaporte. La presencia física no es obligatoria en estos certificados en los casos que marca la ley 59/2003.

- Identificación de la entidad:
  Se exige la identificación de la entidad, para lo que la AR requerirá la documentación pertinente en función del tipo de entidad. Esta información varía dependiendo del tipo de entidad y está incluida en los Manuales operativos de la AR y en la Web de Camerfirma.

- Identificación de la vinculación:

  Para los **Certificados de Apoderamiento Especial y los Certificados de Representación** se exige la documentación sobre la capacidad de representación del Firmante/Suscriptor respecto de la entidad, mediante la entrega de las escrituras notariales que demuestren sus poderes o facultades de representación. Se presentará un certificado expedido por el registro público correspondiente con menos de **10 días** de antigüedad. La AR puede disponer también de medios telemáticos para la consulta en línea del estado y nivel de representación del solicitante.

  En los Certificados de Apoderamiento Especial, las diferentes facultades están descritas en una tabla de epígrafes, las cuales se incorporan en el certificado de dos maneras: una, colocando en el campo CARGO (TITLE) los epígrafes de las facultades de representación, y dos, mediante un link en el campo DECLARACION DEL USUARIO (USER NOTICE) que remite a las escrituras escaneadas y firmadas por el operador de AR. El listado de apoderamientos se puede localizar en: https://www.camerfirma.com/apoderado/poderes.php.

  Para los **Certificados de vinculación** en general, será necesaria la presentación de una autorización firmada por un representante legal o apoderado general de la entidad.

  En los **Certificados de persona jurídica**, en los cuales el Firmante/Suscriptor y el Solicitante son distintos, se deberá demostrar documentalmente que el Solicitante tiene poderes suficientes para realizar dicha solicitud de certificado por cuenta del Firmante/Suscriptor, mediante la presentación de un certificado del registro publico correspondiente no superior a 10 días o mediante consulta en línea realizada por la propia AR a los datos del registro publico correspondiente.

  En los **Certificados de Empleado público** 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. Se exige la documentación 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 AR con su DNI y un documento acreditativo de su pertenencia como empleado a la Administración Publica, organismo o entidad de derecho público donde conste además el NIF de ésta.

En los Certificados Técnicos o de componente:

En los **Certificados de servidor seguro OV (Organization Validation)** se comprueba:

1. La existencia de la entidad mediante el acceso a los registros públicos (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es) o a las bases de datos de la Agencia tributaria (www.aeat.es).

2. La existencia del dominio y el derecho al uso de éste por el suscriptor que se comprueba mediante el acceso a las bases de datos de dominios Internet:

    - http://reports.internic.net
    - 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/

3. El control del dominio por parte de la entidad suscriptora, comprobando que los datos obtenidos en la consulta a las bases de datos de los dominios Internet coinciden claramente con los datos de la entidad presentados en la solicitud.

Dichos certificados se entregan mediante correo electrónico a los responsables administrativo y técnico que aparecen en las bases de datos de dominios.

En los **Certificados de sello electrónico de empresa** se soporta documentalmente mediante la consulta de la existencia de la empresa/entidad, bien en las bases de datos de la AEAT, de Camerdata o de los registros públicos, tal como se hace en la emisión de los Certificados de servidor seguro OV anteriormente visto. El email del solicitante debe proceder de una cuenta de correo cuyo dominio este asociado a la empresa u organismo que ha realizado la solicitud.

El certificado se entregará en dicha dirección de correo. El código de activación en el caso de entregarse un fichero en formato PKCS12 de forma telefónica. El teléfono será localizado accediendo a los servicios de consulta telefónica

https://www.paginasamarillas.es o mediante llamada a servicios de localización de teléfonos. Esta información quedará reflejada en el expediente de emisión del certificado.

En el campo titular de los certificados de sello de empresa puede aparecer: el nombre de la empresa, el nombre del aplicativo para el cual se ha generado el certificado o una referencia interna. Camerfirma no realizará ninguna comprobación sobre estos datos.

Se solicitará para completar el trámite una autorización al solicitante de un representante de la entidad suscriptora, pudiendo ser esta autorización emitida por un departamento jurídico o de recursos humanos.

En los **Certificados de firma de código,** es el mismo mecanismo de comprobación que para la emisión del Certificado de sello electrónico.

En los **Certificados de cifrado** se emitirán de forma telemática utilizando un certificado reconocido valido.

Es posible bajo esta CPS establecer emisiones de certificados de cifrado en procesos de lotes. En estos casos, la comprobación de la identidad puede ser realizada en procesos no presénciales entregando una AR o a Camerfirma, un documento con la identidad del solicitante y su vinculación con una entidad. Este proceso no presencial se realizará solo cuando el certificado permita el uso exclusivo de cifrado.

En los **Certificados de servidor seguro (EV)** *"extended validation"* que siguen las líneas marcadas por *"CA/Browser Forum Gidelines for Issuance and Management of extended validation certificates"*, se realizarán siguiendo los mismos procedimientos que para un Certificado reconocido de vinculación, es decir:

1. La personación física del Firmante/Suscriptor, o de un representante del Solicitante en caso de que éste sea una persona jurídica y la presentación de un documento identificativo.
2. Identificación de la entidad, para lo que la AR requerirá la documentación pertinente dependiendo del tipo de entidad. Debe comprobarse fehacientemente la actividad operativa de la entidad. Esta comprobación se realizara mediante el acceso al registro mercantil o mediante la consulta a otros registros de actividad empresarial del mercado.
3. Presentación de una autorización firmada por un representante de la entidad que actuará como Solicitante..

Además para éstos certificados, la AR deberá comprobar:

4. La existencia de la entidad:
    - Mediante el acceso a los registros públicos (www.registradores.org; www.rmc.es), Camerdata (www.camerdata.es) o a las bases de datos

de la Agencia tributaria (www.aeat.es). En caso de que el operador de AR necesite ampliar la información de la organización incorporada en el certificado, dispondrá de un acceso a una base de datos de gestión de riesgo empresarial como **e-Informa** http://www.einforma.com. Esta base de datos ofrece información del registro mercantil tanto de las empresas como de sus representantes incorporando información de riesgo.

- 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.

5. La existencia del dominio y el derecho al uso de éste por el suscriptor se comprueba mediante el acceso a las bases de datos de dominios Internet:
    - 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/

6. Que la entidad controla el dominio de Internet para el cual se ha emitido el certificado. Es decir que la entidad descrita en el servicio de acceso a la base de datos de dominios Internet está claramente identificada y coincide con la entidad representada por el solicitante del certificado.

Las Guías de emisión de certificadosexigen la diferenciación de tipos de organización diferentes (Privadas, Gobierno, Negocio). En estos casos, el solicitante marca en el documento de solicitud el tipo de entidad a la que pertenece. La autoridad de registro verificará su conformidad y validará el certificado donde se incorporará dicha información tal y como se define en las Guías de emisión de referencia.

Cada tipo de entidad deberá presentar una documentación adecuada a su forma jurídica para demostrar su existencia, según se indica en la página Web de Camerfirma.

Los certificados marcados como EV son comprobados mensualmente por un auditor interno que se asegurará de su correcta emisión y la existencia de la documentación que ha servido de base a su emisión.

En los **Certificados de Sede electrónica para las AAPP y de Sello electrónico para la actuación automatizada** se requerirá la personación física del solicitante. Éste deberá acudir, siempre a instancia de Camerfirma, a la AR correspondiente donde se realizará la comprobación de la documentación acreditativa de los datos contenidos en el formulario de solicitud.

Para los certificados de Sede electrónica se realizarán las mismas comprobaciones que en la emisión de un Certificado de servidor seguro EV ya descritas anteriormente.
Para la emisión de los Certificados de sello electrónico para la actuación automatizada se realizarán las mismas comprobaciones que para un Certificado de sello electrónico de empresa ya descritas anteriormente.

3.2. Renovación de la clave

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

En el caso de los certificados cualificados o reconocidos para firma electrónica no se necesita presencia física ya que la ley de firma LFE 59/2003 permite hasta un periodo de **5 años** desde el último registro presencial, una vez superado este plazo el suscriptor deberá realizar un proceso de emisión presencial.

Los certificados técnicos, es decir servidor seguro, sello empresarial y firma de código, se procede a la renovación de la misma forma que se haría en una emisión nueva.

Camerfirma realizara cuatro avisos al suscriptor vía email de que su certificado va a caducar sugiriendo la realización del proceso de renovación (30 días, 15 días, 7 días, 1). Si su certificado actual caduca antes de realizar la renovación se deberá realizar un proceso de emisión nuevo.

El proceso de renovación se inicial en la página Web de Camerfirma http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Renovar-Certificado.html. Para iniciar el proceso se necesita disponer del certificado activo a renovar.

Una vez identificado en el sistema de renovación, el sistema presenta al suscriptor los datos del certificado antiguo y pide la confirmación de dichos datos. El suscriptor puede modificar solo 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.

Confirmado los datos, el sistema procede a realizar el cobro de los servicios de renovación si estos son pertinentes.

La petición se incorpora al aplicativo de AR donde el operador una vez revisados los datos y el pago, procede a pedir la emisión del certificado a la AC.

La AC emite un nuevo certificado tomando como inicio de validez la finalización del certificado a renovar.

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.

En algunos casos la revocación se produce como consecuencia de un proceso de sustitución del certificado por error en su emisión. En estos casos se reutilizara la documentación soporte entregada para la emisión del certificado sustituido y se elimina la personación física (si se trata de un certificado reconocido) siempre que esta no se haya producido anteriormente al plazo marcado por la ley.

Camerfirma actualizara 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.

3.4. Solicitud de revocación

La forma de realizar las solicitudes de revocación se establecen en el apartado siguiente.

4. Requerimientos Operacionales

4.1. Solicitud de certificados

Las solicitudes de los certificados se realizan mediante el acceso a los formularios de solicitud en la dirección

http://www.camerfirma.com/camerfirmaPublic/index/certificados.html.

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

Se establecen también circuitos de solicitud mediante lotes. En este caso, se enviara por el solicitante a la AR un fichero estructurado según un diseño prefijado por Camerfirma con los datos de los solicitantes. La AR procederá a la carga de dichas peticiones en el aplicativo de AR.

Para la solicitud de certificados también puede realizarse entregando por parte del suscriptor una petición de emisión de certificado estandarizada tipo PKCS#11 o CSR (SSL, certificados de firma de código, certificados de sello de empresa). Se entregara junto con el CSR, si fuera el caso, un documento con los datos adicionales de la petición, los modelos de documentos están publicados en la Web de Camerfirma en el apartado correspondiente a estos tipos de certificados.

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

En los certificados de **empleado público** los procedimientos que se cursan con el nivel alto de aseguramiento es necesaria la identificación inicial con presencia física, ya sea en la solicitud o en la entrega del certificado.

Para los procedimientos que se cursan con el nivel medio de aseguramiento es necesaria la identificación, pero no es imprescindible la presencia física. La identificación se realizará basándose en certificados ya vigentes o en bases de datos administrativas.

En los certificados de **sello electrónico de administración, órgano o entidad de derecho público** es necesaria la identificación de la persona que actúa como responsable del certificado, ya sea en la solicitud o en la entrega del certificado.

En los casos que el certificado Sello electrónico de administración, órgano o entidad de derecho público incorpore un órgano, éste debe identificar su identidad.

4.2. Petición de certificación cruzada.

Camerfirma no tiene actualmente ningún proceso de certificación cruzada activo.

4.3. Emisión de certificados

En certificados Cualificados o Reconocidos: El utiliza un formulario Web para rellenar su solicitud y la confirmación de los datos. En respuesta el aplicativo solicitará mediante un mensaje de correo electrónico al suscriptor la presencia física en las instalaciones de la AR o en un lugar acordado con la documentación correspondiente. Si la solicitud se realiza con un DNI electrónico o con un certificado reconocido admitido por Camerfirma no será necesaria la presencia física.

El operador de AR revisara la documentación del solicitante y comprobara el pago de los servicios si fuera pertinente. Una vez realizadas estas operaciones el operador de AR validara con su firma electrónica la emisión del certificado.

A partir de aquí podemos encontrarnos con los siguientes casos:

Certificados en Software: El usuario recibe en la cuenta de correo asociada al certificado un enlace para 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 o a través de un mensaje SMS conjuntamente con un código de revocación.

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

Certificados en HW: El usuario recibe en las dependencias de la AR el dispositivo de firma con los certificados y las claves generadas. Por otro lado recibirá en la cuenta de correo asociada el código de acceso al dispositivo y el código de desbloqueo, así como una clave de revocación.

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

Certificados en Móvil: Otra opción válida es la emisión del certificado es la entrega de este en un teléfono móvil. Actualmente solo en dispositivos del operador de telefonía Vodafone.

En este caso el suscriptor debe poseer un dispositivo móvil autorizado. AC Camerfirma envía una orden al sistema de gestión del operador telefónico

para que las claves se generen en la tarjeta SIM criptográfica del dispositivo, una vez realizado el sistema de gestión del operador telefónico envía una solicitud PKCS10 a los equipos de Camerfirma, que emiten el certificado correspondiente.

Como se ha comentado anteriormente en este documento, los certificados se pueden solicitar mediante lotes de peticiones. Estos lotes se entregan a la AR por el solicitante en un fichero estructurado que posteriormente introducen en la plataforma de gestión. El operador de AR posteriormente a la recopilación de la documentación y la comprobación de la identidad procederá a realizar la validación de los certificados bien uno a uno o en bloques.

En los certificados técnicos (sello de empresa, Servidor seguro y firma de código) no requieren presencia física para su emisión, solo el envío de la documentación correspondiente a la oficina de AR. Una vez comprobada la documentación y realizado el pago si correspondiera, AC Camerfirma emite un certificado, bien sea mediante la emisión de un fichero PKCS12, o mediante un PKCS7 si el cliente hubiera entregado un PKCS10.

El **Certificado de servidor seguro EV**, requiere según las políticas específicas de este tipo de certificado la presencia física del solicitante en la AR, con la documentación adecuada. El administrador de la AR verifica el pago del servicio, la documentación relativa a la petición y la identidad del Firmante/Suscriptor.

El suscriptor, como hemos dicho anteriormente, podría realizar, con sus propios medios, la generación de las claves en un dispositivo criptográfico y entregar la petición en formato PKCS10 a Camerfirma para emitir el certificado. Este proceso puede establecerse en todos los tipos de certificados pero es común en las peticiones de certificados de servidor seguro donde se aporta un fichero en formato PKCS#10 o CSR.

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

- ✓ Un link a la página donde se generará el certificado en formato PKCS#12.
- ✓ Un PIN necesario para la instalación de las claves y el certificado. El Firmante/Subscritor puede elegir en el formulario de petición el envío mediante SMS.
- ✓ El Firmante/Suscriptor necesitara también para el proceso de creación de las claves y el certificado, un código que estará impreso en el contrato firmado con la AR y la AC.

Si la clave es generada por el suscriptor, este entregara a Camerfirma una petición estandarizada tipo PKCS#10 y Camerfirma enviara al usuario un certificado en formato PKCS#7. Si es el caso el suscriptor deberá entregar a Camerfirma un informe de auditoría confirmando la generación de las claves en un entorno hardware antes de que

Camerfirma emita el certificado, en caso contrario Camerfirma considerara el certificado emitido con dispositivos software.

Para los **Certificados de firma de código, sello electrónico de administración y sello electrónico de empresa,** pueden utilizarse los dos tipos de circuitos ya comentados: Peticiones PKCS#10 y envíos de respuesta en PKCS#7 o envío directo desde Camerfirma del PKCS#12. La AR previamente comprueba los datos a incorporar en el certificado. La AR verificará la exactitud de los datos antes de validarlos para que la CA genere las claves y el certificado asociado.

Los certificados **de Cifrado** se emitirán bien de forma automática, una vez el titular se identifique con un certificado de identidad válido ante la aplicación Web desarrollada al efecto en

http://www.camerfirma.com/camerfirmaPublic/index/certificados/COMPONENTES/CX-Info.html

o bien mediante lotes de solicitudes de certificados, a partir de los cuales Camerfirma emite ficheros PKCS#12.

4.4. Aceptación de certificados.

Un certificado se entenderá aceptado según lo estipulado en las Políticas de certificación.

En general el suscriptor recibe un correo con el link para la descarga del certificado mediante un código de producto mostrado en el proceso de solicitud del certificado.

Si el certificado es en dispositivo hardware el solicitante recibe los dispositivos en la AR, conjuntamente con el material para su instalación.

4.5. Suspensión y revocación de certificados.

4.5.1 Aclaraciones previas

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

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

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).

Los motivos de suspensión de un certificado viene definida 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. Por lo tanto AC Camerfirma solo eliminará de la Lista de revocación un certificados cuando se produzca alguna de las dos siguientes situaciones.

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

4.5.2 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:

Circunstancias que afectan la información contenida en el certificado

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

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 DPC.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor o del responsable de certificado.
- Acceso o utilización no autorizada, por un tercero, de la clave privada del suscriptor o del responsable de certificado.
- El uso irregular del certificado por el suscriptor o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.

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 suscriptor o del responsable de certificado

Circunstancias que afectan el suscriptor o responsable del certificado.

- Finalización de la relación entre Entidad de Certificación y suscriptor o responsable del certificado.
- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o responsable del certificado.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
- Infracción por el suscriptor 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 suscriptor o responsable del certificado.
- La extinción de la persona jurídica suscriptora del certificado, así como la finalidad de la autorización del suscriptor al responsable del certificado o la finalización de la relación entre suscriptor y responsable del certificado.
- Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en esta DPC.

Otras circunstancias

- La suspensión del certificado digital por un periodo superior al establecido en esta DPC.
- La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección en esta DPC.

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

Los suscriptores disponen de los códigos de revocación que pueden usar en los servicios de revocación vía Web o mediante SMS.

4.5.3 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El Firmante/Suscriptor
- El Solicitante responsable
- La Entidad (a través de un representante de la misma)
- La AR ó la AC tras haber autenticado la orden de revocación.

Mas detalles sobre los casos particulares pueden encontrarse en las políticas de certificación concretas.

4.5.4 Procedimiento de solicitud de revocación.

Todas las solicitudes deberán realizarse:

- ✓ A través del Servicio de Revocación ONLINE, accediendo al servicio de revocación localizado en la página de la Web de Camerfirma

  http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Revocar-Certificado.html

- ✓ e introduciendo el PIN de Revocación. Medio de revocación accesible solo para el Firmante/Suscriptor.

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

- ✓ A través del representante suficiente de la Entidad mediante un documento firmado y sellado solicitando la revocación del certificado.

- ✓ 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 solicito la emisión del certificado enviando la solicitud a soporte@camerfirma.com. El operador de Camerfirma confirmara 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.

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 y validación de la solicitud de revocación, Camerfirma revocará definitivamente el certificado.

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

La AR recibirá un correo del sistema informándole que se ha producido una suspensión del certificado.

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

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 ó 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.**

4.5.5 Periodo de revocación

La decisión de revocar o no un certificado se adoptarán en un periodo máximo de **una semana.**

Durante este tiempo el certificado permanece suspendido, mientras se decide si volver a activar la eficacia del mismo ó revocarlo definitivamente basándose en la información obtenida hasta ese momento respecto a las causas que han provocado dicha suspensión.

4.5.6 Suspensión

Ver 4.5.1

4.5.7 Procedimiento para la solicitud de suspensión

La solicitud de suspensión se realizará según el procedimiento descrito en el apartado 4.5.3 de esta CPS.

4.5.8 Límites del periodo de suspensión

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

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

4.5.9 Frecuencia de emisión de CRL's

Ver 2.6.2.

4.5.10 Requisitos de comprobación de CRL's

Los Terceros que confían deben comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida, que podrá descargarse en la siguiente desde su página Web

http://www.camerfirma.com/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

Camerfirma emite CRLs firmadas por Camerfirma que ha emitido el certificado. Es posible que Camerfirma emita si lo considera oportuno CRL firmadas por otra entidad de certificación distinta a la emisora del certificado, lo que se llama un CRL indirecta. En caso

de producirse este hecho Camerfirma lo notificara a través de su página Web, así como los certificados necesarios para la validación de la CRLs emitidas.

El usuario o tercero de confianza deberá comprobar que la lista de revocación es la última emitida.

4.5.11 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/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html

también mediante consultas OCSP en

http://www.camerfirma.com/camerfirmaPublic/index/Servicios/OCSP.html

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 a las que da servicio. 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/camerfirmaPublic/index/Servicios/OCSP.html

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

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**.

4.5.12 Requisitos de la comprobación on-line de la revocación

Para realizar la comprobación de una revocación el Tercero que confía deberá conocer el e-mail asociado al certificado que se desea consultar si se realiza mediante acceso Web y, el número de serie y la autoridad de certificación si se realiza mediante otros mecanismos.

Los requisitos para acceder al servicio **OCSP** y los certificados necesarios para su validación estarán actualizados en la página **http://www.camerfirma.com**

4.5.13 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/camerfirmaPublic/index/Area-Usuario/Consulta-Validacion.html.

Como ejemplo se prestan dos servicios más de comprobación online de certificados:

Consulta del estado de los certificados mediante Web Service según los requerimientos de la AEAT.

Consulta histórica del estado de un certificado. Web Service para consultar el estado de un certificado emitido en la jerarquía JCC en una fecha concreta.

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

No estipulado

4.5.15 Requisitos especiales de revocación por compromiso de las claves

No estipulado

4.6. Procedimientos de Control de Seguridad

Camerfirma está sujeta a las validaciones anuales de la norma ISO27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

4.6.1 Tipos de eventos registrados

Camerfirma registra y guarda los LOG´s de todos los eventos relativos al sistema de seguridad de la AC.
Se registraran 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 LOGs.
- ✓ 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.

4.6.2 Frecuencia de procesado de Logs

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

Camerfirma mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs 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 logs se guardaran en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

4.6.3 Periodos de retención para los LOGs de auditoria

Camerfirma almacena la información de los LOGs al menos durante **5 años**.

4.6.4 Protección de los LOGs de auditoria

Los logs 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 Logs está reservado solo a las personas autorizadas (Auditor).

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 LOGs de auditoría.

4.6.5 Procedimientos de backup de los Logs de auditoria

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

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

Adicionalmente se mantiene copia en centro de custodia externo.

4.6.6 Sistema de recogida de información de auditoria

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de gestión de certificados.

4.6.7 Notificación al sujeto causa del evento

No estipulado.

4.6.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de Camerfirma. Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación ISO27001 que están 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.

4.7. Archivo de registros

4.7.1 Tipo de archivos registrados.

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

- ✓ Todos los datos de auditoría de sistema.
- ✓ Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación.
- ✓ Solicitudes de emisión y revocación de certificados.
- ✓ Todos los certificados emitidos o publicados.
- ✓ CRLs emitidas o registros del estado de los certificados generados.
- ✓ 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.

4.7.2 Periodo de retención para el archivo

Los certificados, los contratos con los Firmantes/Suscriptores y cualquier información relativa a la identificación y autenticación del Firmante/Suscriptor serán conservados durante al menos **15 años**.

4.7.3 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.

4.7.4 Procedimientos de backup 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.

4.7.5 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 tiempos de los equipos utilizados en la emisión de certificados

4.7.6 Sistema de recogida de información de auditoria

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

4.7.7 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.

4.8. Cambio de clave

Antes de que el uso de la clave privada de la AC caduque se realizará un cambio de claves. La vieja AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por la AC vieja. Se generará una nueva AC con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión (ver apartado 3.2. de esta CPS).

4.9. 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.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratara los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

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.

4.9.1 La clave de una entidad se compromete

El Plan de contingencias de Camerfirma trata el compromiso de la clave privada de la AC como una situación de desastre

En caso de compromiso de una clave raíz:

- Informará a todos los Firmantes/Suscriptores, Tercero que confía y otras AC's 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.

4.9.2 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 existente.

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.

4.10. 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 Firmantes/Suscriptores, Tercero que confían y otras AC's 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 logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Las claves privadas de la AC serán destruidas o deshabilitadas para su uso.
- Camerfirma mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.

5. Controles de Seguridad Física, Procedimental y de Personal

Camerfirma está sujeta a las validaciones anuales de la norma ISO27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

5.1. Controles de Seguridad física

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

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.

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.

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 log 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.

5.1.6 Sistema de almacenamiento.

Cada Medio de Almacenamiento desmontable (cintas, cartuchos, disquetes, 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.

5.1.8 Backup externo

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

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

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.

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

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

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

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.

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 backup y mantenimiento de la AC.

Administrador de AR:
Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor.

5.2.2 Número de personas requeridas por tarea

Camerfirma garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes. Principalmente en la manipulación del dispositivo de custodia de las claves de AC Root y AC intermedias.

Nota para certificados de EV

Las políticas de certificación para la emisión de certificados de SSL EV a las que se adhiere esta DPC (*"CA/Browser Forum Gidelines 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 tramite el departamento de auditoria interna de AC Camerfirma revisara esta documentación y procederá a la validación definitiva y la emisión del certificado.

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 AR, para lo cual se activaran o desactivaran 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 paginas.

Modulo de gestión de solicitudes, para lo cual se activara o desactivara los servicios del gestor de páginas específico.

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

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

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

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

El proceso de apagado de módulos seguiría la secuencia:

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

Se realizara el encendido en proceso inverso.

Documentos internos de referencia **IN-2005-05-01 y IN-2008-04-11**

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 esta cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

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

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

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

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**.

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 ISO27001.

Se realizara 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.

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 la 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

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.

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

Para la generación de la clave de las AC's se utiliza un dispositivo que cumple los requerimientos que se detallan en el **FIPS 140-1, en su nivel 3.** Los datos del equipo son: Advanced Crypto Module **(ACM)2** de **RETEMSA**. Se disponen de HSM Eracom con la misma certificación para la emisión de respuestas OCSP y sellos de tiempo.

Camerfirma ha adquirido nuevos módulos criptográficos suministrador por nCipher para sustituir a los actuales de RETEMSA. Estos nuevos módulos albergaran claves raíces nuevas que sustituirán a las actuales.

Las claves correspondientes a la AC que emite certificados de servidor seguro y sello de empresa fueron creadas en un entorno seguro mediante mecanismos software y bajo control dual.

Las claves correspondientes a la AC que emite certificados de servidor EV fueron generadas en un dispositivo criptográfico certificado **FIPS 140-1, en su nivel 3.** Los datos del equipo son: Advanced Crypto Module **(ACM)2** de **RETEMSA**.

Las claves correspondientes a la AC que emite certificados de firma de código (CodeSign) fueron creadas en un dispositivo que cumple los requerimientos que se detallan en el **FIPS 140-1, en su nivel 3.** Los datos del equipo son: Advanced Crypto Module **(ACM)2** de **RETEMSA**.

ROOT **Chambers of Commerce Root**	**2.048**	**34 Años**
CAMERFIRMA	2.048	30 Años
Pertenencia,	1.024	2 Años.
Representante	1.024	2 Años
Persona Jurídica	1.024	2 Años
Apoderado	1.024	2 años
Factura	1.024	2 Años
Cifrado	1.024	Depende del certificado de firma
CAMERFIRMA AAPP	2.048	12 años
De Empleado público Medio	1.024	3 Años

De Empleado público Alto	2.048	3 años
De Sello electrónico de Administración Medio	1.024	3 Años
De Sello electrónico de Administración Alto	2.048	3 Años
De Sede electrónica medio	1.024	3 Años
De Sede electrónica Alto	2.048	3 Años
AC Corporate Server EV	2.048	25 años
Certificado de Servidor	1.024	1,2 años
AC Express Corporate Server	2.048	30 Años
Certificado de Servidor	1.024	1,2,3 Años
AC Sello Electrónico	1.024	1,2,3,4 Años
AC Codesign	2.048	30 Años
Certificado de firma de código	1.024	1,2,3,4 años
AC Sello de tiempo	2.048	30 Años
AC TSU	1.024	5 Años
Token		
AC ROOT-Chambersign Global Root	**2.048**	**34 Años**
CAMERFIRMA	2.048	30 Años
RACER	2.048	20 Años
De servidor de dominio	1.024	1,2,3,4 años
De factura electrónica	1.024	1,2,3,4 años
De persona física	1.024	1,2,3,4 años
De persona física vinculación	1.024	1,2,3,4 años
De Sello empresarial	1.024	1,2,3,4 años
De persona física vinculación Representante	1.024	1,2,3,4 años
De cifrado	1.024	1,2,3,4 años
De persona Jurídica	1.024	1,2,3,4 años
De persona física vinculación apoderamiento	1.024	1,2,3,4 años

Nuevas claves ROOT 2008 para sustituir a las antiguas albergadas en HSM de RETREMSA. Se generaron en una ceremonia de la que existe documentación detallada. Las claves se generaron en los nuevos módulos criptográficos nCipher.

ROOT Chambers of Commerce Root 2008	**4.096**	**30 Años**
AC ROOT-Chambersign Global Root 2008	**4.096**	**30 Años**

6.1.1.1 Generación del par de claves del suscriptor

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

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

Las claves Tienen una longitud mínima de **1024 bits**.

En el caso de que el suscriptor genere las claves en un dispositivo criptográfico propio. Camerfirma exigirá un informe técnico de auditoría que valorará antes de emitir un certificado marcado con claves generadas en dispositivo hardware. Si el suscriptor no aportara el documento o no fuera satisfactorio Camerfirma solo estaría en condiciones de emitir un certificado catalogado como claves generadas en dispositivo software.

6.1.2 Entrega de la clave publica al emisor del certificado

El envío de la clave pública a Camerfirma para la generación del certificado cuando el circuito así lo requiera, se realiza mediante un formato estándar preferiblemente en formato **PKCS#10** o **X509** autoafirmado.

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/camerfirmaPublic/index/Area-Usuario/Claves-Publicas.html

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 suscriptor

Las claves privadas del Firmante/Suscriptor están basadas en el algoritmo **RSA** con una longitud mínima de **1024** bits.

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

6.1.6 Parámetros de generación de la clave pública.

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

6.1.7 Comprobación de la calidad de los parámetros

Longitud del Módulo = 2048
Algoritmo de generación de claves: rsagen1
Método de relleno: emsa-pkcs1-v1_5
Funciones criptográficas de Resumen: SHA-1.

6.1.8 Hardware/software de generación de claves

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

Las claves de las AC´s han sido generadas en un módulo criptográfico Advanced Crypto Module (ACM)2 de RETEMSA acreditado **FIPS-140-1 nivel 3**.

Para las nuevas claves de ROOT 2008 se ha utilizado un nuevo dispositivo criptográfico. nShield PCI 500 F3 de nCipher. Este dispositivo cumple las especificaciones FIPS 140-2 level 2 y level 3.

6.1.9 Fines del uso de la clave

En el siguiente grafico se describe los usos de la clave para los distintos certificados emitidos. La solución adoptada para la diferenciación de usos es la siguiente:

Certificados para autenticación bit DS (puede convivir con otros usos)

Certificados para firma electrónica bit DS + NR (puede convivir con otros usos)

Certificados exclusivos de firma reconocida bit NR (NO puede convivir con otros usos). Actualmente Camerfirma no emite certificados exclusivos de firma electrónica reconocida pero este modelo marca las pautas a seguir en el momento de su incorporación.

AC	DS	NR	KE	DE	KA	KCS	CRLS	EO	DO
ROOT Chambers of Commerce Root						x	x		
CAMERFIRMA	x					x	x		
Pertenencia,	x	x	x*	x*	x				
Representante	x	x	x*	x*	x				
Persona Jurídica	x	x	x*	x*	x				
Apoderado	x	x	x*	x*	x				

Factura	x	x							
Cifrado				x					
CAMERFIRMA AAPP	x					x	x		
Funcionario F		x							
Funcionario A	x								
Funcionario X			x	x					
Funcionario M	x	x	x*	x*					
Sello Admón A	x	x	x	x					
Sello AdmónM	x	x	x	x					
Sede Electr. M	x		x						
Sede Electr. A	x		x						
AC Corporate Server EV						x	x		
Certificado de Servidor	x	x	x	x					
AC Express Corporate Server	x					x	x		
Certificado de Servidor	x	x	x	x					
AC Sello Electrónico	x	x	x	x					
AC Code-Sign	x	x							
AC Sello de tiempo	x					x	x		
TSU	x	x							
AC ROOT-Chambersign Global Root						x	x		
AC CAMERFIRMA	x					x	x		
RACER	x		x*	x*	X*				

DS Firma Digital
NR No Repudio, “ContentCommitment”
KE Cifrado de Clave
DE Cifrado de Datos
KA Acuerdo de clave
KCS Firma de certificados
CRLS Firma de CRL
EO Solo Cifrado
DO Solo descifrado

(*) A pesar de que es posible técnicamente Camerfirma no se responsabiliza de su uso para estos fines

6.2. Protección de la clave privada

Clave privada de la AC

La clave privada de firma de la AC es mantenida y usada en un dispositivo criptográfico seguro que cumple los requerimientos **FIPS 140-1 nivel 3** para las jerarquías **JCC y JCS** y **FIPS 140-1 nivel 2 para las AC´s CP-SP.**

Para la gestión de las claves de las Autoridades de Certificación se utiliza un equipo criptográfico **RETEMSA ACM2 homologado dispositivo FIPS 140-1 nivel 3.**

Para las claves de las autoridades de OCSP y TSA se utiliza un equipo **Eracom certificado FIPS 140-1 nivel 3.**

Cuando al clave privada de la AC está fuera del dispositivo esta se mantiene cifrada y partida en diferentes dispositivos.

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.

Para las nuevas claves de ROOT 2008 se ha utilizado un nuevo dispositivo criptográfico. nShield PCI 500 F3 de nCipher. Este dispositivo cumple las especificaciones FIPS 140-2 level 2 y level 3.

Clave privada del suscriptor

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

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

Respecto a los dispositivos criptográficos con certificados para firma electrónica avanzada, aptas como dispositivos seguros de creación de firma, cumplen el nivel de seguridad CC EAL4+ y soportan los estándares PKCS#11 y CSP.

Camerfirma utiliza como soporte criptográfico aquellos publicados en la siguiente página web:

http://www.bit4id.com/espanol/descargas_camerfirma.htm.

La información respecto al tipo de creación y custodia de claves esta incorporada en el propio certificado digital permitiendo a la Tercero que confía actuar en consecuencia.

6.3. Estándares para los módulos criptográficos

Ver 6.2

6.3.1 Control multipersonal (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.

6.3.2 Custodia de la clave privada

Camerfirma no almacena ni copia claves privadas de los suscriptores cuando estas son generadas por el PSC y están sujetas a la ley de firma 59/2003. Para certificados en soporte hardware es el usuario quien genera y custodia la clave privada en la tarjeta criptográfica entregada por el PSC.

Camerfirma únicamente almacenará una copia de la clave privada del suscriptor cuando esta se use "exclusivamente" para cifrado de datos o aquellos certificados asociados a las claves que no estén sujetas a la ley de firma electrónica 59/2003.

6.3.3 Copia de seguridad de la clave privada

Camerfirma realiza una copia de back up de las claves privadas de la AC's 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 suscriptor 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 suscriptor 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.

6.3.4 Archivo de la clave privada

Las claves privadas de las ACS son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenaran 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 suscriptor 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 publica.

Solo en caso de certificados de cifrado el suscriptor 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.

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.

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

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

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

Las claves asociadas a los suscriptores 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 suscriptor se realiza por medio de un PIN que conocerá solamente el suscriptor y que evitara tenerlo por escrito.

Las claves de la AC se activan por un proceso de m de n. Ver apartado 6.3.1

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

6.3.7 Método de desactivación de la clave privada

La clave privada del suscriptor quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

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

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

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

6.3.8 Método de destrucción de la clave privada

Anteriormente a la destrucción de las claves se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de las AC's 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 suscriptor en software se podrán destruir mediante el borrado de estas siguiendo las instrucciones de la aplicación que las alberga.

Las claves del suscriptor 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.

Documento de referencia: **IN-2006-05-01**-Destrucción Claves de Usuario

6.4. Otros aspectos de la gestión del par de claves

6.4.1 Archivo de la clave pública

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

6.4.2 Periodo de uso para las claves públicas y privadas

Un certificado no debería ser usado después del periodo de validez del mismo aunque el un usuario pueda usarlo para recuperar datos cifrados con la clave publica correspondiente.

6.5. Ciclo de vida del dispositivo seguro de creación de firma.

Los certificados de la AC de las jerarquías **JCC o JCS** se almacenan en un dispositivo seguros de creación de firma **(Hardware)** ó en dispositivo seguro de almacén de datos de creación de firma **(software) q**uedando esta situación reflejada en el contenido del propio certificado.

El dispositivo **software** se entrega en formato **PKCS#12** para importarlo en las aplicaciones. El fichero queda en custodia del suscriptor para su posible recuperación, debiendo guardar los datos de instalación en lugar separado del fichero de claves.

Otro caso de dispositivo software es el empleado en los certificados de servidor seguro donde las claves se generan con los recursos de la aplicación del servidor de paginas.

El dispositivo **hardware** es una tarjeta criptográfica o token USB que cumple los requerimientos de acreditación determinados en la legislación vigente ó al menos **ITSEC E4+.** Estos dispositivos estarán expuestos en la página Web de Camerfirma http://www.bit4id.com/espanol/descargas_camerfirma.htm.

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 suscriptor.
c) El suscriptor o la AR 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 suscriptor o la AR que es introducido en el dispositivo.
e) El dispositivo es reutilizable y puede mantener de forma segura varios pares de claves.

6.6. Controles de seguridad informática

Camerfirma emplea sistemas fiables para ofrecer sus servicios de certificación. Camerfirma ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

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

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

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

6.6.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de Camerfirma incluye las siguientes funcionalidades:

- ✓ control de acceso a los servicios de AC y gestión de privilegios
- ✓ imposición de separación de tareas para la gestión de privilegios
- ✓ identificación y autenticación de roles asociados a identidades
- ✓ archivo del historial del suscriptor y la AC y datos de auditoria
- ✓ auditoria de eventos relativos a la seguridad
- ✓ auto-diagnóstico de seguridad relacionado con los servicios de la AC
- ✓ Mecanismos de recuperación de claves y del sistema de AC

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

6.6.2 Valoración de la seguridad informática

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

6.7. Controles de seguridad del ciclo de vida

6.7.1 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.

6.7.2 Controles de gestión de la seguridad

6.7.2.1 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.

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

6.7.2.2 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.

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.

6.7.2.3 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.

Camerfirma dispone de cajas de seguridad ignifugas para el almacenamiento de soportes físicos.

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.

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.

Planning 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.

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.

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.

6.7.2.4 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.

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

Estado de la revocación

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

6.7.2.5 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 catalogo 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.

6.7.3 Evaluación de la seguridad del ciclo de vida

No estipulado

6.8. Controles de seguridad de la red

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

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

6.9. 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.

6.10. Controles de ingeniería de los módulos criptográficos

Todas las operaciones criptográficas de la AC son realizadas en módulos validados al menos por **FIPS 140-1 nivel 3**.

7. Perfiles de Certificado y CRL

7.1. Perfil de Certificado

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 ETSI 101 867 "Qualified Certificate Profile" .

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 documentos independientes que pueden ser accedidos desde la página Web de Camerfirma. Este método de publicación permite mantener versiones de las políticas y CPS más estables y desligarlos de los muy frecuentes ajustes en los perfiles de los certificados.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es
1. 2. 840. 113549. 1. 1. 5 SHA-1 with RSA Encryption

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

7.1.4 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a 'Distinguished Names' X.500, que son únicos y no ambiguos

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

Todos los certificados tienen un identificador de política que se ajusta al siguiente modelo:

1.3.6.1.4.1.17326.10.X.Y.Z. Para los certificados emitidos por Camerfirma AAPP se ha designado el siguiente OID a requerimiento de las políticas definidas por la Administración del Estado 1.3.6.1.4.1.17326.1.X.Y.Z

X = tipo de certificado
Y = Soporte Hardware o Software.

Z = Generación de la clave PSC o Suscriptor

Para las autoridades de Certificación Raíz e Intermedias se ha definido también un OID de política con el prefijo 1.3.6.1.4.1.17326.10. El OID en las entidades de certificación limita el conjunto de políticas que se encuentran a lo largo de la cadena de certificación. En nuestro caso en toda la cadena debe aparecer el OID 1.3.6.1.4.1.17326.10.

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.

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.

7.3. Perfil de OCSP

Según el estándar RFC 2560.

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 modificara cuando se produzcan cambios relevantes en la gestión de cualquier tipo de certificados sujetos a ella. Se producirán al menos revisiones bienales 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 Firmantes/Suscriptores 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/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html

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.

8.2.2.3 Periodo de comentarios

Los Firmantes/Suscritores y Terceros que confían, afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los **15 días** siguientes a la recepción de la notificación. Las Políticas dicen que 15 días

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/camerfirmaPublic/index/Area-Usuario/Politicas-y-DPC.html

8.4. Procedimientos de aprobación de la CPS

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