DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICAS DE CERTIFICACIÓN

CAMERFIRMA 2021

Versión 1.0.0

Autor: Juan Ángel Martín (Consultor de cumplimiento)

Revisado por: Andrés Vázquez (Dirección de Departamento de Compliance)
France Vidal (Dirección de Departamento Jurídico)

Aprobado por (PA): France Vidal (Dirección de Departamento Jurídico)

Documento válido solo en formato digital firmado electrónicamente por la Autoridad de Políticas (PA).

Este documento se puede obtener en la dirección https://policy2021.camerfirma.com

Idioma: **Castellano**

X2392871C FRANCE MARIE SYLVIA VIDAL (C:A82743287)

X2392871C
FRANCE MARIE
SYLVIA VIDAL
(C:A82743287)
2022.02.21
16:49:28 +01'00'

Índice de Contenido

1. INTRODUCCIÓN

1.1. VISIÓN GENERAL

Dado que no existe una definición inequívoca de los conceptos de Declaración de Prácticas de Certificación y Políticas de Certificación, Camerfirma quiere explicar su postura en relación con estos conceptos, de acuerdo con la RFC 3647 del IETF.

Política de Certificación (en adelante, CP): conjunto de reglas que definen la aptitud de un certificado para una comunidad y/o una aplicación, con unos requisitos de seguridad y uso comunes. En otras palabras, una CP debe definir de forma general la aptitud de los tipos de certificados para determinadas aplicaciones que establecen los mismos requisitos de seguridad y uso.

Declaración de Prácticas de Certificación (en adelante, DPC): conjunto de prácticas adoptadas por una Autoridad de Certificación (en adelante, AC) para la emisión, gestión, revocación y renovación o recodificación de certificados. Suele contener información detallada sobre sus sistemas de seguridad, soporte, administración, emisión (incluida la renovación con y sin cambio de clave) y revocación de certificados, así como la relación de confianza entre el Titular, la tercera parte de confianza y la AC. Puede tratarse de documentos completamente exhaustivos y robustos que proporcionan una descripción precisa de los servicios ofrecidos, procedimientos detallados de gestión del ciclo de vida de los certificados, etc.

Estos conceptos de PC y DPC son diferentes, aunque siguen estando estrechamente relacionados. Una DPC detallada no es una base aceptable para la interoperabilidad de las CA. Las PC son una mejor base para las normas y criterios de seguridad comunes.

En resumen, una PC define "qué" requisitos de seguridad se exigen para la emisión (incluida la renovación con y sin cambio de clave) y la revocación de certificados. La DPC define "cómo" se cumplen los requisitos de seguridad establecidos en la PC.

El Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS) define un "servicio de confianza" como un servicio electrónico prestado normalmente a cambio de una remuneración que consiste en:

(a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

(b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

(c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

El presente documento especifica la DPC y las PC que AC Camerfirma SA (en adelante, Camerfirma) ha establecido para la creación, verificación y validación de los certificados relacionados con la firma electrónica, emitidos por las CA de Camerfirma bajo la jerarquía CAMERFIRMA ROOT 2021, de acuerdo con el Reglamento eIDAS y en base a los siguientes estándares:

Servicio	EN general	EN de alcance	Perfiles/Semántica
Creación, verificación y validación de certificados vinculados con firmas electrónicas	EN 319 401 v2.3.1 General Policy Requirements for Trust Service Providers	EN 319 411-1 v1.3.1: Trust Service Providers issuing certificates; Part 1: General Requirements EN 319 411-2 v2.4.1: Trust Service Providers issuing certificates; Part 2: Requirements for trust	EN 319 412-1 v1.4.4: Certificate Profiles; Part 1: Overview and common data structures EN 319 412-2 v2.2.1: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

		service providers issuing EU qualified certificates	EN 319 412-5 v2.3.1: Certificate Profiles; Part 5: QcStatements

En cuanto a las políticas de certificación que deben aplicarse de acuerdo con ETSI EN 319 411-1 y ETSI EN 319 411-2, se incluyen en las PC descritas en este documento::

- Políticas Generales (ETSI EN 319 411-1):

  NCP Política de certificación normalizada.

  NCP+ Política extendida de certificación normalizada.

- Políticas para certificados cualificados en la UE (ETSI EN 319 411-2):

  QCP-n Política de certificación para los certificados cualificados en la UE emitidos a personas físicas. Incluye todos los requisitos de la política NCP, además de requisitos adicionales adecuados para respaldar la emisión y gestión de certificados cualificados de la UE, tal como se especifica en el Reglamento eIDAS. Los certificados emitidos bajo estos requisitos tienen como objetivo respaldar las firmas electrónicas avanzadas basadas en un certificado cualificado definido en los artículos 26 y 27 del Reglamento eIDAS.

  QCP-n-qscd Política de certificación para los certificados cualificados en la UE emitidos a personas físicas con clave privada asociada a la clave pública certificada en un dispositivo cualificado de creación de firmas electrónicas (en lo sucesivo, QSCD). Incluye todos los requisitos de la política QCP-n (incluidos todos los requisitos de la política NCP+), además de disposiciones adicionales adecuadas para apoyar la emisión y gestión de certificados cualificados de la UE, tal como se especifica en el Reglamento eIDAS, incluidas las específicas de la disposición QSCD. Los certificados emitidos en virtud de estos requisitos están destinados a respaldar las firmas electrónicas cualificadas, tal como se definen en el artículo 3 (12) del Reglamento eIDAS.

Adicionalmente, este documento cumple con la Ley 6/2020 de 11 de noviembre (en adelante, Ley 6/2020) relativa a determinados aspectos de los servicios de confianza electrónica.

El documento está estructurado de acuerdo con la RFC 3647 del IETF.

1.2. IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

Nombre: DPC y CPs Camerfirma 2021

Descripción: Declaración de prácticas de certificación y políticas de certificación para las AC de Camerfirma bajo la jerarquía CAMERFIRMA ROOT 2021

Versión: Ver la página inicial

OIDs
- 1.3.6.1.4.1.17326.10.21.1 (DPC)
- 1.3.6.1.4.1.17326.10.21.1.2.1 (PC CERTIFICADO CUALIFICADO CORPORATIVO - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.2.3 (PC CERTIFICADO CUALIFICADO CORPORATIVO - QCP-n-qscd en QSCD en la nube)
- 1.3.6.1.4.1.17326.10.21.1.3.1 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE LEGAL DE UNA ENTIDAD JURÍDICA - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.3.3 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE LEGAL DE UNA ENTIDAD JURÍDICA - QCP-n-qscd en QSCD en la nube)

- 1.3.6.1.4.1.17326.10.21.1.4.1 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE LEGAL DE UNA ENTIDAD SIN PERSONALIDAD JURÍDICA - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.4.3 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE LEGAL DE UNA ENTIDAD SIN PERSONALIDAD JURÍDICA - QCP-n-qscd en QSCD en la nube)
- 1.3.6.1.4.1.17326.10.21.1.5.1 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE VOLUNTARIO DE UNA ENTIDAD JURÍDICA ANTE LAS ADMINISTRACIONES PÚBLICAS - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.5.3 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE VOLUNTARIO DE UNA ENTIDAD JURÍDICA ANTE LAS ADMINISTRACIONES PÚBLICAS - QCP-n-qscd en QSCD en la nube)
- 1.3.6.1.4.1.17326.10.21.1.6.1 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE VOLUNTARIO DE UNA ENTIDAD SIN PERSONALIDAD JURÍDICA ANTE LAS ADMINISTRACIONES PÚBLICAS - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.6.3 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE VOLUNTARIO DE UNA ENTIDAD SIN PERSONALIDAD JURÍDICA ANTE LAS ADMINISTRACIONES PÚBLICAS - QCP-n-qscd en QSCD en la nube)
- 1.3.6.1.4.1.17326.10.21.1.7.1 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE ESPECIAL DE UNA PERSONA JURÍDICA - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.7.3 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE ESPECIAL DE UNA PERSONA JURÍDICA - QCP-n-qscd en QSCD en nube)
- 1.3.6.1.4.1.17326.10.21.1.8.1 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE GENERAL DE UNA ENTIDAD SIN PERSONALIDAD JURÍDICA - QCP-n-qscd en QSCD SmartCard o Token)
- 1.3.6.1.4.1.17326.10.21.1.8.3 (PC CERTIFICADO CUALIFICADO PARA UN REPRESENTANTE GENERAL DE UNA ENTIDAD SIN PERSONALIDAD JURÍDICA - QCP-n-qscd en QSCD en nube)

Localización: https://policy21.camerfirma.com

1.3. PARTICIPANTES EN LA PKI

1.3.1. AUTORIDADES DE CERTIFICACIÓN (ACS)

Una AC es un componente de una PKI responsable de la emisión y gestión de certificados digitales. Una AC es un tipo de proveedor de servicios de confianza (TSP) que emite certificados digitales. Actúa como tercera parte de confianza entre el Sujeto y la Parte que Confía en las transacciones digitales, asociando una clave pública específica con el Sujeto. La AC tiene la responsabilidad última en la prestación de servicios de certificación.

La AC emisora se identifica en el campo Emisor de cada certificado digital.

La AC emisora se identifica en el campo Emisor de cada certificado digital.

Bajo esta DPC, una AC pertenece a la persona jurídica especificada en el atributo organización (O) del campo Emisor de los certificados digitales emitidos por esta AC.

Bajo esta DPC, Camerfirma actúa como ACs con los siguientes datos corporativos:

Nombre Corporativo:	AC CAMERFIRMA, S.A.
NIF:	A82743287
Domicilio Social:	calle Ribera del Loira 12 - 28042 Madrid
Teléfono:	+34 91 344 37 43
Email:	ca@camerfirma.com

Página Web: https://www.camerfirma.com

Desde mayo de 2018, Camerfirma es propiedad de la empresa italiana InfoCert, S.p.A., sujeta a la gestión y coordinación de TINEXTA, S.p.A. (página web: https://www.infocert.it).

Una AC utiliza Autoridades de Registro (en adelante, AR) con el fin de comprobar y almacenar la documentación del contenido de los certificados digitales de las entidades finales. Conforme a la actual DPC, las ACs pueden desempeñar el trabajo de las ARs en cualquier momento.

Un TSP puede incorporar una o más jerarquías de AC. Una jerarquía de ACs incluye una AC raíz y una o más ACs intermedias (también conocidas como ACs subordinadas).

El uso de jerarquías de ACs reduce los riesgos que conlleva la emisión de certificados y su organización en las diferentes ACs. Las claves de las ACs intermedias se gestionan en un entorno en línea más ágil, mientras que las claves de la AC raíz se gestionan en un entorno fuera de línea más seguro.

Una AC intermedia obtiene un certificado de la AC raíz para emitir certificados de entidad final u otros certificados de AC intermedia. El número de ACs intermedias permitidas bajo una AC Raíz o Intermedia se especifica en la extensión *Basic Constraints* (*pathLenConstraint*) del certificado de la AC.

A continuación se describe la jerarquía de ACs que Camerfirma gestiona como propietaria (bien directamente o a través de filiales) bajo esta DPC. En el caso de ACs intermedias propiedad de otra organización, esta DPC hace referencia a su existencia dentro de la jerarquía correspondiente debido a su subordinación a la AC Raíz, pero se regirá por su propia DPC.

Como característica general, los nombres de las AC en los certificados emitidos para ellas incorporan el año de emisión del certificado. Por ejemplo, el nombre de la AC puede cambiar para incluir el año de emisión de un nuevo certificado al final del nombre, aunque las características seguirán siendo las mismas, a menos que se indique lo contrario en esta DPC.

Bajo esta DPC, Camerfirma gestiona la siguiente jerarquía de ACs:

- CAMERFIRMA ROOT 2021

1.3.1.1. JERARQUÍA CAMERFIRMA ROOT 2021

Esta jerarquía de ACs está diseñada para desarrollar una red de confianza, con el objetivo final de emitir certificados digitales dentro de la Unión Europea, y en la que las AR son gestionadas por las Cámaras de Comercio, Industria y Navegación españolas u otras entidades públicas o privadas.

Los datos de identificación del certificado de la AC raíz de esta jerarquía son:

CN: CAMERFIRMA ROOT 2021

Válido desde (hora UTC): 19/10/2021 12:26:35

Válido hasta (hora UTC): 13/10/2045 12:26:35

Número de Serie: 34 61 2C A9 B6 C3 7A 12 FE 65 50 A0 6B 28 EE EC EE BA F3 E4

***X509v3 Subject Key Identifier*:** 51 11 32 7A 10 D0 D8 8C 4C 09 84 97 B1 A9 3E B2 54 BA 87 C9

***Hash SHA-1*:** 33 9F 6E F0 37 AA EE BA A0 CE 54 80 06 02 DD FB 18 6C 1C EE

***Hash SHA-256*:** AD FC 94 10 EE 0D 10 91 EE FD 5C DD FA E5 65 1E 3B 1D 66 B6 9C 0D AB C5 9E 33 91 B3 58 5A 53 8E

The scheme of Intermediate Certification Authorities issuing digital certificates under this hierarchy is:

CAMERFIRMA ROOT 2021
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021

1.3.6.1.4.1.17326.10.21.1.2.1 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO CORPORATIVO - QCP-n-qscd en QSCD SmartCard o Token
1.3.6.1.4.1.17326.10.21.1.2.3 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO CORPORATIVO - QCP-n-qscd en QSCD en la nube
1.3.6.1.4.1.17326.10.21.1.3.1 [Camerfirma] 2.21.724.1.3.5.8 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN - QCP-n-qscd en QSCD SmartCard o Token
1.3.6.1.4.1.17326.10.21.1.3.3 [Camerfirma] 2.21.724.1.3.5.8 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN - QCP-n-qscd en QSCD en la nube
1.3.6.1.4.1.17326.10.21.1.4.1 [Camerfirma] 2.21.724.1.3.5.9 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN - QCP-n-qscd en QSCD SmartCard o Token
1.3.6.1.4.1.17326.10.21.1.4.3 [Camerfirma] 2.21.724.1.3.5.9 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN - QCP-n-qscd en QSCD en la nube
1.3.6.1.4.1.17326.10.21.1.5.1 [Camerfirma] 2.21.724.1.3.5.8 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA TRÁMITES CON LAS AAPP - QCP-n-qscd en QSCD SmartCard o Token
1.3.6.1.4.1.17326.10.21.1.5.3 [Camerfirma] 2.21.724.1.3.5.8 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA TRÁMITES CON LAS AAPP - QCP-n-qscd en QSCD en la nube
1.3.6.1.4.1.17326.10.21.1.6.1 [Camerfirma] 2.21.724.1.3.5.9 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA TRÁMITES CON LAS AAPP - QCP-n-qscd en QSCD SmartCard o Token

1.3.6.1.4.1.17326.10.21.1.6.3 [Camerfirma] 2.21.724.1.3.5.9 [requisito de la Administración Pública Española] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA TRÁMITES CON LAS AAPP - QCP-n-qscd en QSCD en la nube
1.3.6.1.4.1.17326.10.21.1.7.1 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA APODERADOS - QCP-n-qscd en QSCD SmartCard o Token
1.3.6.1.4.1.17326.10.21.1.7.3 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA APODERADOS - QCP-n-qscd en QSCD en nube
1.3.6.1.4.1.17326.10.21.1.8.1 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA APODERADOS - QCP-n-qscd en QSCD SmartCard o Token
1.3.6.1.4.1.17326.10.21.1.8.3 [Camerfirma] 0.4.0.194112.1.2 [eIDAS QCP-n-qscd]	CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA APODERADOS - QCP-n-qscd en QSCD en nube

Todas las ACs de Camerfirma pueden emitir certificados respondedores de OCSP que se utilizarán para firmar las respuestas del servicio OCSP sobre el estado de los certificados emitidos por las ACs. El OID de los certificados respondedores OCSP emitidos por todas las ACs de Camerfirma es 1.3.6.1.4.1.17326.10.21.0.1

1.3.1.1.1. AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021

AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021 es una CA intermedia multi-política, que puede emitir certificados cualificados para personas físicas y jurídicas (actualmente, sólo para personas físicas) dentro de la UE, y de acuerdo con los requisitos del Reglamento eIDAS y la Ley 6/2020.

Los datos de identificación de este certificado de CA (emitido por la CA Raíz de la jerarquía CAMERFIRMA ROOT 2021):

CN: AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021

Válido desde (hora UTC): 20/10/2021 15:12:16

Válido hasta (hora UTC): 16/10/2037 15:12:16

Número de Serie: 1C 20 0D 92 11 23 B8 98 38 0F C2 B9 24 19 BB A9 9B 94 C2 C2

***X509v3 Subject Key Identifier*:** C7 6F 2D C4 10 8A 6E DD F3 11 65 69 C6 4A 43 7B

***Hash SHA-1*:** 2E 0F 6F 10 E6 14 5E 50 57 FC 03 B2 53 C5 00 6E E0 6D 19 EE

***Hash SHA-256*:** 4D 18 7D 4E 5B BA 7B BA D4 22 B7 5B EF B4 DC B2 17 9D 1C CD 11 5A 18 D2 C8 35 0F FF AC 31 6B 34

Los certificados de entidad final emitidos por esta CA están destinados a:

1.3.1.1.1.1. PERSONAS FÍSICAS CON UNA RELACIÓN EMPRESARIAL CON UNA ENTIDAD

1.3.1.1.1.1.1. CERTIFICADO DE CORPORATIVO CUALIFICADO – QCP-N-QSCD

Este certificado identifica a una persona física (Titular/Sujeto/Firmante) y determina como atributos específicos, el tipo de relación contractual (laboral, comercial, institucional, etc.) entre una persona física (Titular/Sujeto/Firmante) y una Entidad (campo de organización del certificado).

1.3.1.1.1.1.2. CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN – QCP-N-QSCD.

Este certificado identifica a una persona física (Titular/Sujeto/Firmante) y determina como atributos específicos, su condición de representante legal o apoderado con plenas facultades, con capacidad para actuar en nombre de una Persona Jurídica.

Está dirigido a representantes legales de entidades con personalidad jurídica como Administrador Único, Administrador Solidario, Consejero Delegado, etc., y a apoderados con plenas facultades de representación (similares a las de un representante legal) que les permita actuar tanto en el ámbito de las relaciones y trámites con las Administraciones Públicas (usos de autenticación y firma) como en el ámbito de la contratación de bienes o servicios o relativos al funcionamiento ordinario de la entidad (usos de firma).

Los representantes legales mancomunados o los apoderados mancomunados que deseen solicitar este certificado para uno de ellos, deberán ostentar poderes que incluyan, al menos, la facultad solidaria de representación de la Entidad Jurídica para sus relaciones y trámites con las Administraciones Públicas.

En todo caso, el Titular/Sujeto/Firmante del certificado es el encargado de utilizarlo de acuerdo con sus Poderes y la parte que confía de verificar su contenido y alcance.

1.3.1.1.1.1.3. CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN – QCP-N-QSCD.

Este certificado identifica a una persona física (Titular/Sujeto/Firmante) y determina como atributos específicos, su condición de representante legal o representante con plenas facultades, con capacidad para actuar en nombre de una Entidad sin Personalidad Jurídica.

Está dirigido a representantes legales de Entidades sin Personalidad Jurídica como Administrador Único, Administrador Solidario, Director/Gerente, Presidente de Propietarios, etc., y a apoderados con plenas facultades de representación (similares a las de un representante legal) que les permita actuar tanto en el ámbito de las relaciones y trámites con las Administraciones Públicas (usos de autenticación y firma) como en el ámbito de la contratación de bienes o servicios o relativos al funcionamiento ordinario de la entidad (usos de firma).

Los representantes legales mancomunados o los apoderados mancomunados que deseen solicitar este certificado para uno de ellos, deberán ostentar poderes que incluyan, al menos, la facultad solidaria de representación de la Entidad sin Personalidad Jurídica para sus relaciones y trámites con las Administraciones Públicas.

En todo caso, el Titular/Sujeto/Firmante del certificado es el encargado de utilizarlo de acuerdo con sus Poderes y la parte que confía de verificar su contenido y alcance.

1.3.1.1.1.1.4. CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA TRÁMITES CON LAS AAPP – QCP-N-QSCD.

La finalidad de este certificado es identificar a una persona física (Titular/Sujeto/Firmante) y determinar como atributos específicos, su capacidad para representar a una Entidad Jurídica en el ámbito de sus relaciones con las Administraciones Públicas (usos de autenticación y firma).

Está dirigido a apoderados con Poder General o Poder Específico que incluya al menos facultades que les permitan realizar, en nombre de la Entidad Jurídica, actuaciones y trámites ante las Administraciones Públicas que requieran el uso de la firma electrónica o del certificado electrónico.

Los representantes legales mancomunados o los apoderados mancomunados que quieran solicitar este certificado, deberán ostentar poderes que incluyan al menos la facultad solidaria de representación de la Persona Jurídica para sus

relaciones y trámites ante las Administraciones Públicas. Alternativamente, pueden aportar un Poder específico, o un documento fehaciente firmado por todos los apoderados conjuntamente a favor de uno de ellos.

En todo caso, el Titular/Sujeto/Firmante del certificado es el encargado de utilizarlo de acuerdo con sus Poderes y la parte que confía de verificar su contenido y alcance.

1.3.1.1.1.1.5. CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA TRÁMITES CON LAS AAPP – QCP-N-QSCD.

La finalidad de este certificado es identificar a una persona física (Titular/Sujeto/Firmante) y determinar como atributos específicos, su capacidad para representar a una Entidad sin Personalidad Jurídica en el ámbito de sus relaciones con la Administración Pública (usos de autenticación y firma).

Está dirigido a apoderados con Poder General o Poder Específico que incluya al menos facultades que les permitan realizar en nombre de la Entidad sin Personalidad Jurídica actuaciones y trámites ante las Administraciones Públicas que requieran el uso de la firma electrónica o del certificado electrónico.

Los representantes legales mancomunados o los apoderados mancomunados que quieran solicitar este certificado, deberán ostentar poderes que incluyan al menos la facultad solidaria de representación de la Entidad sin Personalidad Jurídica para sus relaciones y trámites ante las Administraciones Públicas. Alternativamente, pueden aportar un Poder específico, o un documento fehaciente firmado por todos los apoderados conjuntamente a favor de uno de ellos.

En todo caso, el Titular/Sujeto/Firmante del certificado es el encargado de utilizarlo de acuerdo con sus Poderes y la parte que confía de verificar su contenido y alcance.

1.3.1.1.1.1.6. CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA APODERADOS – QCP-N-QSCD.

Este certificado identifica a una persona física (Titular/Sujeto/Firmante) y determina como atributos específicos, su capacidad para actuar en nombre de una Persona Jurídica sólo para determinadas facultades enmarcadas en su función/departamento (usos de firma).

Este certificado no es recomendable para usos de autenticación en plataformas de la Administración Pública por la limitación implícita de los poderes cuyo alcance exacto no puede conocer la parte que confía.

Los apoderados mancomunados pueden solicitar este certificado si aportan un Poder especifico o un documento fehaciente firmado por todos los apoderados conjuntamente a favor de uno de ellos.

En cualquier caso, el Titular/Sujeto/Firmante del certificado es el encargado de utilizarlo de acuerdo con sus facultades y la parte que confía de verificar su contenido y alcance.

1.3.1.1.1.1.7. CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA APODERADOS – QCP-N-QSCD.

Este certificado identifica a una persona física (Titular/Sujeto/Firmante) y determina como atributos específicos, su capacidad para actuar en nombre de una Persona sin Personalidad Jurídica sólo para determinadas facultades enmarcadas en su función / departamento (usos de firma).

Este certificado no es recomendable para usos de autenticación en plataformas de la Administración Pública por la limitación implícita de los poderes cuyo alcance exacto no puede conocer la parte que confía.

Los apoderados mancomunados pueden solicitar este certificado si aportan un Poder especifico, o un documento fehaciente firmado por todos los apoderados conjuntamente a favor de uno de ellos.

En cualquier caso, el Titular/Sujeto/Firmante del certificado es el encargado de utilizarlo de acuerdo con sus facultades y la parte que confía de verificar su contenido y alcance.

1.3.1.2. EMISIÓN DE CERTIFICADOS DE PRUEBAS

Camerfirma emite certificados con datos ficticios para que las ACs los faciliten a los organismos reguladores en los procesos de inspección, acreditación o registro de nuevos certificados, así como a los desarrolladores de aplicaciones para que los utilicen en el proceso de integración o evaluación para la aprobación del certificado. Camerfirma incluye en estos

certificados la siguiente información para que la parte que confía pueda ver claramente que se trata de un certificado de pruebas sin garantía:

Nombre de la entidad: [SOLO PRUEBAS]/[TEST ONLY] ENTIDAD
Nº de identificación fiscal de la entidad: R0599999J
Nombre: JUAN ANTONIO
Primer Apellido: CÁMARA
Segundo Apellido: ESPAÑOL
Nº de identificación nacional: 00000000T
CN: [SOLO PRUEBAS]/[TEST ONLY] ...

Cuando un proceso requiere la emisión de un certificado de pruebas con datos reales, éste se realiza sólo tras la firma de un acuerdo de confidencialidad con la entidad responsable del proceso. En este caso, los datos son propios de cada cliente, pero antes siempre aparece el nombre de la entidad '[SOLO PRUEBAS]' o '[TEST ONLY]' para identificar a simple vista que se trata de un certificado de prueba sin garantía.

1.3.2. AUTORIDADES DE REGISTRO (ARS)

Una AR puede ser una persona física o jurídica que actúa de acuerdo con esta DPC y, en su caso, mediante un acuerdo con una AC concreta, ejerciendo las funciones de gestión de solicitudes, identificación y registro de solicitantes de certificados, y cualquier otra responsabilidad establecida para las PCs concretas en este documento. Las AR son autoridades delegadas por las AC intermedias, aunque éstas son las responsables últimas del servicio.

Según la actual DPC, se reconocen los siguientes tipos de AR:

- RA Camerales: Las gestionadas directamente o bajo el control de una Cámara de Comercio, Industria y Navegación española.
- RA Corporativas: Son las gestionadas por un organismo público o una entidad privada para distribuir certificados a sus trabajadores.

A efectos de esta DPC, puede actuar como AR de las AC intermedias propiedad de AC Camerfirma:

- La AC.
- Las Cámaras de Comercio, Industria y Navegación españolas, o las entidades que éstas designen. Las entidades delegadas pueden llevar a cabo el proceso de registro.
- Empresas españolas, como entidades delegadas por la AR de la AC o por las AR de las Cámaras de Comercio, Industria y Navegación españolas, a las que están asociadas contractualmente, para realizar la completa identificación y registro del Solicitante, dentro de una determinada organización o demarcación. Con carácter general, los operadores de estas AR Corporativas sólo gestionan el servicio en el ámbito de su organización o demarcación, salvo que la AR de la que dependen determine lo contrario. Por ejemplo, los empleados de una corporación, los miembros de un grupo empresarial, los miembros de un colegio profesional.
- Entidades pertenecientes a las AAPP españolas.
- Otras personas jurídicas o agentes, españoles o internacionales, que tengan una relación contractual con las AC y hayan superado los procesos de registro. Están obligadas a realizar con éxito las auditorías exigidas en el contrato según el PC. Para la emisión de certificados a personas físicas o jurídicas que no residan en territorio español, se podrá exigir un informe jurídico que justifique el correcto cumplimiento de los requisitos de identificación y registro.

A su vez, la AR puede delegar parcialmente en una tercera persona/entidad denominada Punto de Verificación Presencial (PVP) las tareas de identificación:

- PVP. Punto de Verificación Presencial que depende siempre de una AR. Su misión principal es identificar al solicitante mediante un método presencial y entregar a la AR las pruebas de la identificación. La AR comprueba las pruebas y, si son correctas, valida de acuerdo con el procedimiento de expedición aplicable.
  En ocasiones, las funciones de las PVP pueden ampliarse a la recopilación de la documentación presentada, la comprobación de su adecuación al tipo de certificado solicitado y la entrega de la SmartCard o Token Solicitante en su caso, pero una PVP nunca puede validar el proceso de registro y decidir la emisión del certificado.

Camerfirma ha elaborado un documento tipo de relación entre la AR y el PVP donde se definen las funciones que la AR delega en el PVP.

1.3.3. SUSCRIPTORES Y SUJETOS/TITULARES

Bajo esta DPC y de acuerdo con la ETSI EN 319 401, el Suscriptor es la persona física o jurídica vinculada por un acuerdo con Camerfirma que actúa como CA ante cualquier obligación del Suscriptor.

Bajo esta DPC y según ETSI EN 319 411-1, el Sujeto es el Titular del certificado (titular de la clave privada asociada a la clave pública del certificado) y se encuentra descrito en el campo *Subject* del certificado.

Bajo esta DPC y de acuerdo con el Reglamento eIDAS, el Sujeto/Titular de un certificado de firma electrónica es una persona física denominada el *Firmante*, y el Sujeto/Titular de un certificado de sello electrónico es una persona jurídica denominada el *Creador del sello*.

Bajo las PC descritas en este documento el Sujeto/Titular puede ser:

- Una persona física asociada a una organización.

Bajo las PC descritas en este documento el Suscriptor puede ser:

- La organización a la que está asociada la persona física Sujeto/Titular.
- La persona física Sujeto/Titular.

Para evitar un conflicto de intereses, Camerfirma no podrá ser Suscriptor de certificados electrónicos salvo que emita para sí misma (como persona jurídica) o para personas físicas que formen parte de ella (como Sujeto) y salvo los casos en los que una tercera organización ejecute todas o parte de las tareas de AR para emitir certificados para sujetos identificados en asociación con ella. En ambos casos la solicitud, validación y tramitación debe realizarse según los procesos definidos por Camerfirma.

1.3.4. PARTE QUE CONFÍA

En este documento, la Parte que Confía es la persona que recibe una transacción digital realizada con un certificado emitido por cualquiera de las AC de Camerfirma incluidas en este documento y que confía voluntariamente en el Certificado que la AC emite.

1.3.5. OTROS PARTICIPANTES

1.3.5.1. ENTIDAD DE ACREDITACIÓN U ORGANISMO DE SUPERVISIÓN.

El Organismo de Supervisión es la entidad de gestión correspondiente que acepta, acredita y supervisa a los TSP dentro de un área geográfica determinada. Dentro de España, esta tarea corresponde al Ministerio de Asuntos Económicos y Transformación Digital, que es la autoridad competente según el Estado español miembro del Espacio Económico Europeo.

Las AC intermedias que no son propiedad de Camerfirma pueden estar sujetas a marcos legales en diferentes países o regiones. En estos casos, el Organismo de Supervisión se refiere al organismo nacional correspondiente.

1.3.5.2. PRESTADOR DE SERVICIOS DE CONFIANZA (TSP)

Según el Reglamento eIDAS, un proveedor de servicios de confianza (TSP) es una persona física o jurídica que presta uno o varios servicios de confianza, ya sea como proveedor de servicios de confianza cualificado o no cualificado.

Según el Reglamento eIDAS, un Proveedor de Servicios de Confianza Cualificado (QTSP) es un TSC que presta uno o más servicios de confianza cualificados y al que el Organismo de Supervisión le concede el estatus de cualificado.

Los servicios de confianza definidos en el Reglamento eIDAS incluyen:

- La creación, verificación y validación de firmas electrónicas. Se incluyen los certificados relativos a estos servicios.
- La creación, verificación y validación de sellos electrónicos. Se incluyen los certificados relativos a estos servicios.
- La creación, verificación y validación de sellos de tiempo electrónicos. Se incluyen los certificados relativos a estos servicios.
- Servicios de entrega electrónica certificada. Se incluyen los certificados relativos a estos servicios.
- La conservación de firmas electrónicas, sellos o certificados relacionados con dichos servicios.

1.3.5.3. ENTIDAD/ORGANIZACIÓN

En el marco de las DPC y PC descritas en este documento, la Entidad es una organización pública o privada, individual o colectiva, reconocida por la ley, con la que la persona física/Sujeto/Titular/Firmante mantiene una determinada relación, definida en el campo ORGANIZACIÓN (O) de cada certificado. Según el caso, puede ser el Suscriptor (apartado 1.3.3 o no).

1.3.5.4. SOLICITANTE

En el marco de esta DPC, se entiende por Solicitante el Sujeto/Titular cuando éste es una persona física, y la persona física que realiza la solicitud de certificado en nombre del Sujeto/Titular cuando éste es una persona jurídica.

En las PC descritas en este documento, se entiende por Solicitante el Sujeto/Titular.

1.3.5.5. RESPONSABLE DEL CERTIFICADO

Para los certificados emitidos a personas físicas, esta DPC y las PC descritas en este documento consideran al Sujeto/Titular como Responsable del certificado (responsable de la clave privada asociada a la clave pública del certificado).

Para los certificados emitidos a personas jurídicas, sin perjuicio de las obligaciones del Sujeto/Titular, esta DPC considera al Solicitante, o a una persona física autorizada por el Solicitante, como Responsable del certificado (responsable de la clave privada asociada a la clave pública del certificado).

1.4. USOS DEL CERTIFICADO

1.4.1. USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados para personas físicas o jurídicas emitidos en el marco de estas políticas se utilizan para los siguientes propósitos

- Autenticación del Sujeto/Titular del Certificado.
- Firma electrónica, avanzada o cualificada cuando se utiliza con dispositivos cualificados de creación de firma electrónica.
- Cifrado asimétrico o mixto sin recuperación de claves.

1.4.2. USOS PROHIBIDOS Y NO AUTORIZADOS DE LOS CERTIFICADOS

Camerfirma incluye información sobre la limitación de uso en el certificado, bien en campos normalizados en los atributos "*key usage*", "*basic constraints*" marcados como críticos en el certificado y por tanto obligatorios para las aplicaciones que lo utilizan, o bien limitaciones en atributos como "*extended key usage*", "*name constraints*" y/o a través de textos incluidos en el campo "*issuer's statement*" (*user notice*) marcados como "*non-critical*" pero obligatorios para el titular y usuario del certificado.

Los certificados sólo pueden utilizarse para los fines para los que fueron emitidos y están sujetos a los límites definidos en este documento.

Los certificados no están concebidos, no pueden utilizarse y no están autorizados para su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran acciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o sistemas de comunicación aérea o de control de armas, en los que un fallo podría provocar directamente la muerte, lesiones personales o daños medioambientales graves.

El uso de los certificados digitales en transacciones que contravengan las PC aplicables a cada uno de los Certificados, la CPS o los Términos y Condiciones que las ACs firman con las ARs y con los Suscriptores/Sujetos se considera ilegal, quedando las ACs exentas de cualquier responsabilidad por el uso indebido de los certificados por parte del Firmante o de un tercero de acuerdo con la legislación vigente.

Camerfirma no tiene acceso a los datos para los que se utiliza un certificado. Por tanto, debido a la falta de acceso al contenido de los mensajes, Camerfirma no puede emitir ninguna valoración sobre estos contenidos y el Firmante es por tanto responsable de los datos para los que se utiliza el certificado. El Firmante es también responsable de las consecuencias de cualquier uso de estos datos contrario a las limitaciones y condiciones establecidas en este documento y en los Términos y Condiciones que las ACs firman con el Sujeto/Firmante, así como de cualquier uso indebido de los mismos de acuerdo con este apartado o que pueda ser interpretado como tal en virtud de la legislación vigente.

La clave privada de los certificados es almacenada por Camerfirma únicamente para el certificado en QSCD Cloud, por lo que no es posible recuperar los datos cifrados con la clave pública correspondiente en caso de pérdida de la clave privada del certificado por parte del titular del mismo. Si el titular cifra los datos con la clave pública, lo hace bajo su única y exclusiva responsabilidad.

1.5. AUTORIDAD DE POLÍTICAS

Para las jerarquías aquí descritas, la Autoridad de Políticas le compete al departamento legal de Camerfirma.

1.5.1. ORGANIZACIÓN QUE ADMINISTRA ESTE DOCUMENTO

La redacción y revisión de este documento es realizada por los departamentos de Cumplimiento y Jurídico de Camerfirma en colaboración con los departamentos de Operaciones y Sistemas.

1.5.2. DATOS DE CONTACTO

Dirección: Calle Ribera del Loira, 12. Madrid (España)

Teléfono: +34 91 344 37 43

Email: compliance@camerfirma.com

Página Web: https://www.camerfirma.com

En cuanto al contenido de esta DPC y PCs, se considera que el lector está familiarizado con los conceptos básicos de PKI, certificación y firma digital. En caso de que el lector no esté familiarizado con estos conceptos, puede informarse en la página web de Camerfirma https://www.camerfirma.com, donde se puede encontrar información general sobre el uso de la firma digital y los certificados digitales.

Para comunicar incidencias de seguridad relacionadas con los certificados por parte del TSP, puede contactar con Camerfirma a través de incidentes@camerfirma.com.

1.5.3. PERSONA QUE DETERMINA LA IDONEIDAD DE DPC PARA LA POLÍTICA

El departamento jurídico de Camerfirma constituye, pues, la Autoridad de Políticas (AP) de las jerarquías de la AC descritas anteriormente siendo responsable de la idoneidad de las DPC y las PC de este documento.

1.5.4. PROCEDIMIENTO DE APROBACIÓN DE LA DPC

La publicación de las revisiones de este documento debe ser aprobada por la AP que corresponde al departamento legal de Camerfirma.

Camerfirma publica cada nueva versión de este documento en su página web https://policy21.camerfirma.com. La DPC se publica en formato PDF firmado electrónicamente con el certificado digital del aprobador.

1.6. SIGLAS Y DEFINICIONES

1.6.1. SIGLAS

AgID	*Agenzia per l'Italia Digitale*. Agencia para Italia Digital.
AP	Autoridad de Políticas.
AR	Autoridad de Registro.
AWS	Servicios Web de Amazon.
AC	Autoridad de Certificación.
CAB	Organismo de Evaluación de Conformidad.
CC	Criterios Comunes.

CN	Nombre común.
PC	Política de Certificación.
DPC	Declaración de Prácticas de Certificación.
CRL	Lista de certificados revocados.
CSR	Solicitud de firma de certificado.
DMZ	Zona desmilitarizada.
DN	Nombre Distinguido.
DNI	Documento Nacional de Identidad.
DSCF	Dispositivo Seguro de Creación de Firmas.
EAL	Nivel de Garantía de Evaluación.
EEA	Área Económica Europea.
eIDAS	*electronic Identification, Authentication and trust Services*.
EN	Estándares Europeos.
ETSI	Instituto de Estándares Europeos de Telecomunicaciones.
UE	Unión Europea.
FIPS	Publicación de la Normativa Federal de Tratamiento de la Información
GLONASS	Sistema global de navegación por satélite.
GPS	Sistema de posicionamiento global.
HSM	Modulo de Seguridad Hardware.
HTTP	Protocolo de Transferencia de Hipertexto.
IEC	Comisión Electrotécnica Internacional.
IETF	*Internet Engineering Task Force*. Grupo de Trabajo de Ingeniería de Internet
INRIM	Instituto Nacional de Investigación Metrológica de Italia.
ISO	Organización Internacional de Normalización.
ITU	Unión Internacional de Telecomunicaciones.
MPLS	*Multiprotocol Label Switching*.
NAS	*Network-Attached Storage*.
NCP	Política de Certificación Normalizada.

NCP+	Política de Certificación Normalizada Extendida.
NIE	Número de Identidad de Extranjero.
NTP	*Network Time Protocol*.
Número de IVA	Número de Identificación del Impuesto del Valor Añadido.
O	Organización.
OCSP	*On-line Certificate Status Protocol*. Protocolo para la consulta del estado de los certificados.
OID	*Object Identifier*. Identificador de Objeto.
OTP	*One-time password*. Contraseña de un solo uso.
PadES	*PDF Advanced Electronic Signatures*.
PDF	*Portable Document Format*.
PIN	*Personal Identification Number*.
PKCS#10	El más común de los formatos de CSRs.
PKI	*Public Key Infrastructure*. Infraestructura de Clave Pública.
PVP	Punto de Verificación Presencial.
QCP-n	Política de UE Certificados Cualificados emitidos a personas naturales.
QCP-n-qscd	Política de UE Certificados Cualificados emitidos a personas naturales de los que la claves privada y el certificado asociados están en un QSCD.
QSCD	*Qualified electronic Signature/Seal Creation Device*. Dispositivo Cualificado de Creación de Firmas/Sellos Electrónicos.
QTSP	*Qualified Trusted Service Provider*.
RFC	*Request for Comments* de IETF.
RGPD	*General Data Protection Regulation* (EU) 2016/679.
RSA	*Rivest-Shamir-Adleman*. Tipo de algoritmo criptográfico.
RTO/RPO	*Recovery Time Objective*/*Recovery Point Objective*.
SHA	*Secure Hash Algorithm*. Algoritmo Seguro de *Hash*.
SSL	*Secure Sockets Layer*. Un protocolo diseñado por Netscape que se ha convertido en un estándar en Internet. Permite la transmisión de información encriptada entre un navegador y un servidor.
STS	Protocolo *Station-to-Station*.
TIN	*Tax Identification Number*. Número de Identificación para Impuestos.
TS	Especificación Técnica de ETSI.

TSP	*Trusted Service Provider*. Proveedor de Servicios de Confianza.
UPS	*Uninterruptible Power Supply*. Sistema de alimentación ininterrumpida.
UTC	Hora Universal Coordinada.

1.6.2. DEFINICIONES

Autoridad de Certificación	Es la entidad responsable de la emisión y gestión de los certificados digitales. Actúa como tercero de confianza entre el Sujeto/Firmante y la Parte que Confía, asociando una clave pública específica con una persona.
Autoridad de Políticas	Persona o grupo de personas responsables de todas las decisiones relativas a la creación, gestión, mantenimiento y retirada de las políticas de certificación y DPC.
Autoridad de Registro	Es la entidad responsable de la gestión de las solicitudes y de la identificación y registro de los certificados. A los efectos de esta DPC, la denominación de "Autoridad de Registro" o "AR" se aplicarán ambos en referencia a las AR de Camerfirma.
Certificado	Un archivo que asocia la clave pública con unos datos que identifican al Sujeto/Firmante y que están firmados por la AC.
Clave privada	Valor matemático que sólo conoce el Sujeto/Firmante y que se utiliza para crear una firma digital o descifrar datos. También se denominan datos de creación de la firma. La clave privada de la AC se emplea para firmar los certificados y las CRLs.
Clave pública	Valor matemático conocido públicamente que se utiliza para verificar una firma digital o cifrar datos. También se denominan datos de verificación de la firma.
CRL	Un archivo que contiene una lista de certificados que han sido revocados en un determinado periodo de tiempo y que está firmado por la CA.
Datos de Activación	Datos privados como los PIN o las contraseñas utilizadas para activar la clave privada.
DPC	Se define como un conjunto de prácticas adoptadas por una AC para emitir certificados de acuerdo con una política de certificación específica.
DSCF	Dispositivo Seguro de Creación de Firma. Elemento de software o hardware utilizado por el Sujeto/Firmante para la generación de firmas digitales, de manera que las operaciones criptográficas se realizan dentro del dispositivo y el control está garantizado únicamente por el Sujeto/Firmante.
Entidad	En el contexto de estas políticas de certificación, una empresa u organización de cualquier tipo con la que el Solicitante tenga algún tipo de relación.
Firma Digital	El resultado de la transformación de un mensaje, o de cualquier tipo de datos, por parte de la aplicación privada en conjunción con algoritmos conocidos, garantizando de esta forma: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (ID) c) que la persona que firma los datos no pueda negar haberlo hecho (no repudio en origen)

Firma electrónica cualificada	Es una firma electrónica que cumple con el Reglamento de la UE Nº 910/2014 (Reglamento eIDAS) para las transacciones electrónicas en el mercado interior europeo. Permite verificar la autoría de una declaración en el intercambio de datos electrónicos durante largos períodos de tiempo. Las firmas electrónicas cualificadas pueden considerarse un equivalente digital a las firmas manuscritas.
Firma Electrónica Avanzada	una firma electrónica que cumpla los requisitos especificados en el artículo 26 del Reglamento eIDAS: (a) está vinculado de forma inequívoca al firmante ; (b) es capaz de identificar al firmante; (c) se crea utilizando datos de creación de la firma electrónica que el firmante puede, con un alto nivel de confianza, utilizar bajo su exclusivo control; y (d) está vinculada a los datos firmados con ella de tal manera que cualquier cambio posterior en los datos es detectable.
OID	Un identificador numérico único registrado en el marco de la normalización ISO y que se refiere a un objeto o clase de objeto concreto.
Par de Claves	Conjunto formado por una clave pública y otra privada, ambas relacionadas entre sí matemáticamente.
Parte que Confía	En el contexto de esta política de certificación, la persona que voluntariamente confía en el certificado digital y lo utiliza como medio para acreditar la autenticidad e integridad del documento firmado.
PKI	Conjunto de dispositivos y elementos de hardware, software, recursos humanos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de Certificación	Un conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en una aplicación, con requisitos comunes de seguridad y uso.
Proveedor de Servicios de Confianza	Una persona física o jurídica que presta uno o varios servicios de confianza, ya sea como proveedor cualificado o como proveedor no cualificado de servicios de confianza.
Proveedor de Servicios de Confianza Cualificado	Un proveedor de servicios de confianza que presta uno o más servicios de confianza cualificados y que ha sido reconocido como cualificado por el Organismo de Supervisión.
Servicio de Confianza	es un servicio electrónico prestado por un TSP que puede consistir en: (a) la creación, verificación, validación de firmas electrónicas o sellos electrónicos o sellos de tiempo electrónicos. También puede tratarse de servicios de entrega electrónica certificada y de certificados relacionados con estos servicios; (b) la creación, verificación y validación de certificados para la autenticación de sitios web; (c) la conservación de firmas electrónicas, sellos o certificados relacionados con estos servicios.

Servicio de Confianza Cualificado	Un servicio de confianza que cumple con los requisitos establecidos en el Reglamento eIDAS.
Solicitante	En el contexto de esta política de certificación, el solicitante es una persona física con poderes especiales para llevar a cabo determinados procedimientos en nombre de la entidad.
Sujeto/Firmante	En el contexto de esta declaración de prácticas de certificación, la persona física cuya clave pública está certificada por la AC y que tiene una clave privada válida para generar firmas digitales.

2. RESPONSABILIDAD DE PUBLICACIÓN Y REPOSITORIOS

2.1. REPOSITORIOS

Los repositorios de Camerfirma para la publicación de la información de certificación están disponibles 24 horas al día, 7 días a la semana.

2.2. PUBLICACIÓN DE INFORMACIÓN

2.2.1. POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN

Camerfirma pone a disposición del público sus DPC y PC en https://policy21.camerfirma.com.

2.2.2. TÉRMINOS Y CONDICIONES

El Sujeto, y el Suscriptor si son personas distintas, reciben información sobre los Términos y Condiciones que deben aceptar antes de la emisión del certificado. Las Partes que Confían también pueden consultar los Términos y Condiciones en el sitio web de Camerfirma:

- https://www.camerfirma.com/tc/terminos_y_condiciones21.pdf (Español)
- https://www.camerfirma.com/tc/terms_and_conditions21.pdf (Inglés)

2.2.3. DIFUSIÓN DE LOS CERTIFICADOS

Camerfirma pone a disposición del público su certificado de AC Raíz 'CAMERFIRMA ROOT 2021' en http://ca.camerfirma.com/certs/camerfirmaroot2021.crt.

Camerfirma pone a disposición del público su certificado de AC Intermedia 'AC CAMERFIRMA QUALIFIED CERTIFIATES - 2021' en http://ca.camerfirma.com/certs/camerfirmaqc2021.crt.

Es responsabilidad del Sujeto entregar su certificado a cualquier persona que solicite comprobar la validez de su certificado.

2.2.4. LISTAS DE REVOCACIÓN Y OCSP

Las listas de revocación se publican en el registro público de certificados, al que se puede acceder a través del protocolo HTTP, tal y como se indica en los "*CRL Distribution Points*" del certificado. Se puede acceder a las listas a través de productos conformes disponibles en el mercado que puedan interpretar el protocolo HTTP.

Las ACs pueden proporcionar opciones de acceso adicionales para consultar la lista de certificados publicados y su validez.

El principal servicio de las ACs de consulta de estado de un certificado es el ofrecido por OCSP.

Camerfirma pone a disposición su servicio OCSP en: http://ocsp2021.camerfirma.com/.

2.3. FRECUENCIA DE PUBLICACIÓN

Se creará una nueva versión de este documento al menos una vez al año. Camerfirma publica inmediatamente en su web cualquier cambio en este documento, manteniendo un histórico de versiones del mismo.

Las versiones antiguas de los documentos se conservan durante un periodo mínimo de quince (15) años y pueden ser consultadas por los interesados en su página web https://policy21.camerfirma.com.

La AC emite y publica periódicamente listas de revocación de acuerdo con el apartado 4.9.7.

2.4. CONTROL DE ACCESO A LOS REPOSITORIOS

Camerfirma pone a disposición del público su repositorio.

Camerfirma utiliza sistemas fiables para el repositorio, de forma que:

- Se pueda comprobar la autenticidad de los certificados. El propio certificado a través de la firma de la AC garantiza su autenticidad.
- Personas no autorizadas no puedan alterar los datos. La firma digital de la AC protege contra la manipulación de los datos incluidos en el certificado.
- El solicitante puede autorizar o no la publicación del certificado en el proceso de solicitud.

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. DENOMINACIÓN

3.1.1. TIPOS DE NOMBRES

El Sujeto/Firmante aparece descrito por un nombre distintivo (DN, *distinguished name*, *Subject*) de acuerdo con la norma X.500. Los certificados se emiten de acuerdo con la especificación IETF RFC 5280 y ETSI EN 319 412 Partes 2 y 3.

Las descripciones de los campos DN se muestran en cada una de las fichas de los perfiles de los certificados. También incluye un componente de "*Common Name*" (CN =).

Véase la sección 7.1 para obtener información sobre las fichas de perfiles.

La estructura y el contenido de los campos de cada certificado emitido por Camerfirma, así como su significado semántico, se describen en cada ficha de perfil de los certificados.

- Personas físicas: En los certificados correspondientes a personas físicas, la identificación del Firmante se realiza con su nombre completo y NIF.
- La estructura para las ACs intermedias, los certificados OCSP incluyen al menos:
    - Un nombre descriptivo que identifica a la AC (CN)
    - La entidad legal responsable de las claves (O)
    - El número de identificación fiscal de la organización responsable de las claves (OrganizationIdentifier)
    - El país en el que la empresa responsable de las claves desarrolla su actividad (C)
- Los certificados de AC Raíz tienen un nombre descriptivo que identifica a la AC y el campo (O) contiene el nombre de la organización responsable de la AC.

3.1.2. NECESIDAD DE QUE LOS NOMBRES SEAN SIGNIFICATIVOS

Todos los DN deben ser significativos, y la identificación de los atributos asociados al suscriptor debe estar en una forma legible para las personas. Véase la sección 7.1.4 Formato de los nombres.

3.1.3. ANONIMATO O PSEUDÓNIMOS DE SUSCRIPTORES

Los suscriptores no pueden utilizar seudónimos.

3.1.4. REGLAS PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

Camerfirma se ajusta a la norma ISO/IEC 9594 X.500 y a IETF RFC 5280.

3.1.5. UNICIDAD DE LOS NOMBRES

Dentro de una misma CA, un *Distinguished Name* de un Sujeto que ya ha sido tomado no puede ser reasignado a un Sujeto diferente. Esto se garantiza incluyendo el código de identificación fiscal único a la cadena de nombres que distingue al titular del certificado.

3.1.6. RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE MARCAS REGISTRADAS Y OTROS SIGNOS DISTINTIVOS

Camerfirma no asume ninguna obligación en cuanto a la emisión de certificados en relación con el uso de marcas u otros signos distintivos. Camerfirma no permite deliberadamente el uso de un signo distintivo en el Sujeto/Titular/Firmante que no tenga derechos de uso. Sin embargo, las ACs no están obligadas a solicitar pruebas sobre los derechos de uso de marcas u otros signos distintivos antes de emitir los certificados.

3.1.7. PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS DE NOMBRES

Camerfirma no es responsable en caso de resolución de conflictos de nombres. En cualquier caso, los nombres se asignan de acuerdo con el orden en que se registran.

Camerfirma no arbitrará este tipo de conflictos, que las partes deberán resolver directamente entre ellas.

3.2. VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1. MÉTODO DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

Las claves creadas por Camerfirma bajo PCs descritas en este documento:

- En Hardware: Las claves pueden ser entregadas por Camerfirma al Sujeto/Titular/Firmante, directamente o a través de una RA en un dispositivo cualificado de creación de firma (QSCD).
- En almacenamiento remoto centralizado: Camerfirma utiliza un sistema de almacenamiento remoto de claves, permitiendo al Sujeto/Firmante acceder a la clave desde diferentes dispositivos. Las claves se almacenan en un dispositivo HSM FIPS-104-2 nivel 3 o EAL4+ asegurando el control único de esta clave por parte del Sujeto/Firmante (QSCD).

3.2.2. IDENTIFICACIÓN DE LA ENTIDAD

3.2.2.1. IDENTIDAD

Antes de la emisión y entrega de un certificado emitido a una persona física con el atributo de estar vinculada a una entidad, es necesario verificar los datos relativos a la constitución y personalidad jurídica de la entidad.

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

En el caso de entidades fuera del territorio español, la documentación a aportar será la del Registro Oficial del país correspondiente, debidamente apostillada y con traducción jurada en lengua española indicando la existencia de la entidad en dicho país.

Las agencias de registro empleadas para la identificación de organizaciones en España son

- Registro Mercantil
- Agencia Tributaria
- Agencia de Registro específica según el tipo de entidad.

En las administraciones públicas: La documentación que acredita la existencia de la administración pública, organismo público o entidad pública no es necesaria porque esta identidad forma parte del ámbito institucional de la Administración General del Estado o de otra Administración Pública Estatal.

3.2.2.2. MARCAS REGISTRADAS

Véase la sección 3.1.6.

3.2.2.3. VERIFICACIÓN DEL PAÍS

Véase la sección 3.2.2.1.

3.2.2.4. VALIDACIÓN DE LA AUTORIZACIÓN O CONTROL DE DOMINIO

Las ACs incluidas en este DPC no emiten certificados SSL/TLS.

3.2.2.5. AUTENTICACIÓN DE UNA DIRECCIÓN IP

Las ACs incluidas en este DPC no emiten certificados SSL/TLS.

3.2.2.6. VALIDACIÓN DE DOMINIO *WILDCARD*

Las ACs incluidas en este DPC no emiten certificados SSL/TLS.

3.2.2.7. EXACTITUD DE LAS FUENTES DE DATOS

Véase la sección 3.2.2.1.

3.2.2.8. CAA

Las ACs incluidas en este DPC no emiten certificados SSL/TLS y por lo tanto no hay requisitos sobre incorporación a CAA.

3.2.3. IDENTIFICACIÓN DE LA IDENTIDAD DE UN INDIVIDUO

Documento de identidad: Antes de la emisión y entrega de un certificado, se requiere la verificación de la identidad personal del Solicitante. El Solicitante debe presentar su Documento de Identidad original en vigor, de acuerdo con los siguientes requisitos:

Nacionalidad española:

- Documento Nacional de Identidad o Pasaporte.

Extranjeros de la UE o del EEE:

- Pasaporte o Documento de Identidad expedido por un país de la UE o del EEE y Certificado de Número de Identidad de Extranjero (NIE).

Extranjeros de otros países residentes en España:

- Tarjeta de Residencia o Tarjeta de Identidad de Extranjero con fotografía.

Extranjeros de otros países no residentes en España:

- Pasaporte.

En el caso de los documentos de identidad extranjeros, deben presentarse con la Apostilla de la Haya y, si se considera necesario, con una traducción oficial.

No se podrán expedir certificados a menores no emancipados, incapacitados legal o parcialmente, o cuando existan sospechas razonables de que el Solicitante no está en posesión de sus plenas capacidades mentales.

El control de la dirección de correo electrónico incorporada en la solicitud del certificado se verifica mediante la comunicación de un valor aleatorio que se exigirá en el momento de la generación y descarga del certificado. Esta comprobación será realizada exclusivamente por la AC, por lo que no puede ser delegada.

Métodos de Identificación: la identidad de una persona se verificará mediante uno de los métodos indicados en el Reglamento eIDAS y de conformidad con la legislación nacional aplicable:

1. Presencia física: se requiere la presencia física del Solicitante ante un Operador de la Autoridad de Certificación, un Operador de la Autoridad de Registro o un Punto de Verificación Física presencial. El Solicitante puede optar por acudir a un Notario Público y presentar la solicitud de emisión del certificado con su firma autenticada.
2. De forma remota, utilizando medios de identificación electrónica para los que, antes de la emisión del certificado cualificado, se haya garantizado la presencia física de la persona natural y que cumplan los requisitos establecidos en el artículo 8 en relación con los niveles de garantía "sustancial" o "alto" (del Reglamento eIDAS). Se aceptarán los sistemas de identificación electrónica especificados por los Estados miembros en el artículo 9.1 del Reglamento eIDAS. En España se aceptará el DNI electrónico.
3. Mediante otro certificado cualificado de firma electrónica emitido por una AC de Camerfirma u otro Proveedor, para el que la persona física se haya identificado personalmente o utilizando medios de identificación electrónica de acuerdo con el punto 2 anterior, siempre que los datos de identidad de la persona física (y, en su caso, los atributos del certificado solicitado) estén contenidos en el certificado utilizado.
4. O bien, mediante la utilización de otros métodos de identificación reconocidos a nivel nacional que ofrezcan una garantía de fiabilidad equivalente a la de la presencia física, de acuerdo con la normativa aplicable, en particular las condiciones y requisitos técnicos establecidos en la Orden ETD/465/2021, de 6 de mayo, del Ministerio de Asuntos Económicos y Transformación Digital, por la que se regulan los métodos de video identificación a distancia para la expedición de certificados electrónicos cualificados. La identificación del Solicitante puede

realizarse de forma asistida, con la mediación sincrónica de un operador, o de forma no asistida, sin interacción en línea entre un operador y el Solicitante, pero con una revisión posterior por parte de un operador.

Camerfirma pone a disposición de sus usuarios, diversos procesos de identificación remota por vídeo, que pueden ser utilizados para la emisión de certificados electrónicos reconocidos, siempre que cumplan con las condiciones y requisitos técnicos exigidos por la normativa aplicable, que deben ser confirmados en un Informe de Evaluación de la Conformidad emitido por un Organismo de Evaluación de la Conformidad, en concreto los siguientes:

- Proceso asistido con mediación sincrónica de un operador.
- Proceso asistido con validación previa de la documentación y mediación sincrónica de un operador.
- Proceso desasistido sin interacción en línea con un operador, pero con revisión posterior por parte de un operador.

En todos los procesos, se aplicarán las siguientes medidas adicionales:

- Si el Solicitante ha presentado un DNI o NIE, Camerfirma deberá consultar los datos de identidad del Solicitante a través de la plataforma de intermediación del Servicio de Verificación y Consulta de Datos que el Organismo de Control pone a su disposición, siempre que los requisitos técnicos de la plataforma y el soporte de acreditación del DNI o NIE lo permitan.
- Los datos de registro, es decir, los archivos de audio y vídeo y los metadatos estructurados en formato electrónico, se almacenan de forma protegida y de acuerdo con la norma europea sobre protección de datos personales.
- Por razones de seguridad y prevención del fraude, sólo se aceptarán documentos de identidad convencionales en esta modalidad de identificación (DNI español y pasaportes españoles o extranjeros). La identificación de los Solicitantes extranjeros que no dispongan de Pasaporte, podrá ser autorizada por la AC previa revisión de las características objetivas de sus documentos de identidad en cuanto a certeza de identificación, seguridad de la AC y formación específica.

Lo dispuesto en este apartado sobre la obligación de verificar la identidad y demás características de los Solicitantes de un certificado reconocido podrá no ser exigido cuando la identidad u otros atributos permanentes de los Solicitantes del certificado ya sean conocidos por Camerfirma o la AR en virtud de una relación preexistente, en la que, para la identificación del interesado, se hayan utilizado los medios indicados en el punto 1 y el periodo de tiempo transcurrido desde la identificación sea inferior a cinco años.

3.2.4. INFORMACIÓN DE SUSCRIPTOR NO VERIFICADA

No está permitido incluir información no verificada en el "*Subject*" de un certificado.

3.2.5. VALIDACIÓN DE LA AUTORIDAD

3.2.5.1. IDENTIFICACIÓN DE LA VINCULACIÓN

Tipo de Certificado	Documentación
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN - QCP-n-qscd CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN - QCP-n-qscd CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA TRÁMITES CON LAS AAPP - QCP-n-qscd	Acreditar las facultades de representación del Sujeto/Firmante frente a la entidad, aportando la documentación que acredite sus facultades de representación en función del tipo de entidad. Esta información está publicada en los manuales de operación de la AR y en la web de Camerfirma.

Tipo de Certificado	Documentación
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA TRÁMITES CON LAS AAPP - QCP-n-qscd CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA APODERADOS - QCP-n-qscd CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA APODERADOS - QCP-n-qscd	
CERTIFICADO CUALIFICADO CORPORATIVO - QCP-n-qscd	Normalmente, una autorización firmada por el Representante Legal de la entidad.

Según el artículo 24.2.h) del Reglamento eIDAS, esta actividad de registro puede realizarse por medios electrónicos, tanto si los documentos aportados son documentos electrónicos válidos como si son documentos en papel. En este último caso, el Operador de Registro deberá conservar una copia escaneada y firmarla digitalmente con su Certificado Digital, para su conservación en archivos informáticos.

3.2.5.2. IDENTIDAD DEL SERVICIO O MÁQUINA

Las ACs incluidas en este DPC no emiten certificados SSL/TLS.

3.2.5.3. CONSIDERACIONES SOBRE LA IDENTIFICACIÓN DE LOS INDIVIDUOS QUE OCUPAN PUESTOS DE ALTA DIRECCIÓN

Camerfirma utiliza procedimientos especiales para la identificación de los individuos que ocupan puestos de alta dirección en empresas y administraciones para la emisión de certificados digitales. En estos casos, un Operador de Registro se desplaza a las instalaciones de la organización para asegurar la presencia física del titular del certificado. Para la identificación de la relación entre el titular del certificado y la organización representada en la administración pública, se suele utilizar la publicación de los cargos en los Boletines Oficiales del Estado.

3.2.5.4. CONSIDERACIONES ESPECIALES PARA LA EMISIÓN DE CERTIFICADOS FUERA DEL TERRITORIO ESPAÑOL

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

3.2.6. CRITERIOS PARA LA INTEROPERACIÓN

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

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA LAS SOLICITUDES DE RENOVACIÓN CON CAMBIO DE CLAVE

La solicitud de renovación con cambio de clave de un certificado es el proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado cuando su fecha de caducidad está próxima, el certificado ha caducado o ha sido revocado.

3.3.1. IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RENOVACIÓN CON CAMBIO DE CLAVE RUTINARIA

La identificación de una solicitud de renovación con cambio de clave puede realizarse utilizando los mismos métodos que para la validación de la identidad inicial (sección 3.2), incluido el uso del certificado que se va a renovar, o si la identidad del solicitante u otras circunstancias permanentes y la identificación del interesado se han llevado a cabo en persona hace menos de cinco años.

3.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN PARA RENOVACIÓN CON CAMBIO DE CLAVE DESPUÉS DE LA REVOCACIÓN

Una vez que un certificado ha sido revocado, no puede ser renovado automáticamente. El solicitante debe iniciar un nuevo procedimiento de emisión.

Excepción: Cuando la renovación con cambio de clave se produce en certificados de entidad final debido a un proceso de sustitución del certificado o a un error de emisión o a una pérdida, el certificado puede renovarse tras una revocación, siempre y cuando demuestre la condición actual. Se reutiliza la documentación justificativa presentada para la emisión del certificado sustituido y no es necesaria la presencia física, si se requiere habitualmente por la naturaleza del certificado, si éste se emitió hace menos de cinco años.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN

El método de presentación de solicitudes de revocación se establece en el apartado 4.8 de este documento.

Camerfirma, o cualquiera de las entidades que la componen, podrá, por iniciativa propia, solicitar la revocación de un certificado si tiene conocimiento o sospecha de que la clave privada del suscriptor ha sido comprometida, o si tiene conocimiento o sospecha de cualquier otro hecho que aconseje tomar dicha medida.

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

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Las solicitudes de certificados cualificados para personas físicas deben ser presentadas por el Solicitante (véase la sección 1.3.5.4):

4.1.2. PROCESO DE SOLICITUD DE CERTIFICADOS Y RESPONSABILIDADES

El proceso de registro incluye la solicitud del Solicitante, la identificación, la entrega de documentación adicional relacionada con la entidad y la condición de representante (podría ser incluida), la generación del par de claves, la solicitud de certificado de clave pública y la firma del contrato (no necesariamente en ese orden).

Cada parte implicada en el proceso tiene responsabilidades específicas y contribuye conjuntamente en el éxito de la emisión del certificado:

- El Solicitante/Sujeto es responsable de proporcionar información correcta y veraz sobre su identidad y sobre los atributos específicos del Sujeto, de leer cuidadosamente el material puesto a disposición por la AC -incluso a través de la AR- y de seguir las instrucciones de la AC y/o de la AR al presentar una solicitud de certificado cualificado. Si el Sujeto es una persona jurídica, estas responsabilidades recaen sobre el representante legal o el apoderado que presenta la solicitud de certificado cualificado;
- El Suscriptor, si está presente, es responsable de informar al Sujeto en cuyo nombre solicita un certificado sobre las obligaciones derivadas del mismo, así como de proporcionar información correcta y veraz sobre la identidad del Sujeto y de seguir los procedimientos e indicaciones dadas por la AC y/o la AR;
- La AR, si está presente, es responsable -incluso a través del Operador de Registro- de la identificación del Sujeto o de la identificación del Suscriptor si el Sujeto es una persona jurídica, y de la exactitud y validez de los atributos del Sujeto (en caso de certificado con atributos), informándole de las obligaciones derivadas del certificado y siguiendo con detalle los procesos definidos por la AC;
- La AC es la responsable última de la identificación del Sujeto/Suscriptor, la verificación de los atributos y el registro exitoso del certificado calificado.

4.2. PROCESAMIENTO DE LAS SOLICITUDES DE CERTIFICADOS

Para obtener un certificado de firma, el Sujeto y/o el Suscriptor deben:

- Leer detenidamente esta DPC, los Términos y Condiciones y cualquier material informativo adicional;
- Cumplir con los procedimientos de identificación adoptados por la AC, tal y como se describe en la sección 3.2.3;
- Proporcionar toda la información requerida para la identificación junto con cualquier documentación apropiada (cuando se requiera);

- Proporcionar toda la información requerida para la existencia y validez de los atributos junto con cualquier documentación apropiada (cuando se requiera)
- Firmar la solicitud de registro y certificación y aceptar las condiciones contractuales que rigen la prestación del servicio, utilizando los correspondientes formularios analógicos o electrónicos establecidos por la AC.

La información que debe proporcionar el Sujeto:

- Persona física. En el caso de que se solicite un certificado para una persona física, el Sujeto y/o el Suscriptor deberán facilitar la siguiente información
    - Apellidos y nombre
    - Fecha y lugar de nacimiento;
    - Código fiscal o código de identificación similar (TIN).
    - Dirección de residencia;
    - Referencias del documento de identidad utilizado para la identificación (por ejemplo, tipo de documento, número, emisor y fecha de emisión);
    - Una dirección de correo electrónico para el envío de comunicaciones de la AC al Sujeto;
    - Un número de teléfono móvil para el envío de OTP, cuando se utilice esta tecnología OTP.

  La dirección de email y el número de teléfono móvil facilitados a la AR, deberán ser válidos e identificar de forma única al Sujeto. La dirección de email se utilizará para cualquier comunicación de la AR y para el envío de códigos de emergencia (ERCs) y avisos de caducidad.

- Persona jurídica. En caso de que se solicite un certificado para una persona jurídica, el Suscriptor que actúe como representante legal o apoderado de la persona jurídica deberá facilitar la siguiente información:
    - Apellidos y nombre del suscriptor;
    - Código fiscal o código de identificación similar (TIN) que posee el Suscriptor;
    - Datos del documento utilizado para la identificación del suscriptor (por ejemplo, tipo de documento, número, emisor y fecha de emisión);
    - Una dirección de email para la transmisión de comunicaciones de la AC al Suscriptor;
    - Nombre del Sujeto (persona jurídica);
    - Número de IVA.

- Atributos específicos. En caso de que se solicite un certificado para una persona física con atributos específicos relacionados con su relación empresarial con una entidad:
    - Cargo o puesto en la entidad (opcional)
    - Departamento 1
    - Departamento 2 (opcional)

- Atributos específicos. En caso de que se solicite un certificado para una persona física con atributos específicos relacionados con su condición de representante/apoderado de una entidad:
    - Cargo o puesto en la entidad (opcional)
    - Departamento 1
    - Departamento 2 (opcional)
    - Escritura pública / Poderes

La información proporcionada se almacena en los archivos de la AC (fase de registro) y sirve de base para la generación del certificado cualificado.

4.2.1. EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Durante la fase de registro inicial y recogida de las solicitudes de registro y certificación, el Sujeto o el Suscriptor que actúa como representante legal de una persona jurídica recibe un código de seguridad que le permite activar el dispositivo de firma o el proceso de firma si es de forma remota. Los códigos de seguridad se entregan en un sobre de seguridad o, si son electrónicos, se transmiten en archivos cifrados.

La AC puede establecer que el PIN de firma sea seleccionado de forma independiente por el Sujeto o Suscriptor que representa legalmente a una persona jurídica. En estos casos, es responsabilidad del Sujeto/Suscriptor recordar el PIN.

La AC también puede disponer que el certificado de firma remota pueda ser utilizado a través de un sistema de autenticación proporcionado por la AR, que tenga un nivel de seguridad como mínimo significativo, o que sea proporcionado, tras analizar las características del propio sistema, dentro del ámbito de certificación del dispositivo seguro de firma. En estos casos, el sistema de autenticación puede utilizarse también para cualquier solicitud de revocación del certificado.

4.2.2. APROBACIÓN O RECHAZO DE SOLICITUDES

Tras el registro inicial, la AC o la AR pueden negarse a completar la emisión de un certificado de firma por falta de información o por información incompleta, por verificaciones de concordancia y contra el fraude, cuando la identidad del Sujeto/Suscriptor no está clara, etc.

4.2.3. PLAZO PARA RESOLVER LA SOLICITUD

El tiempo que transcurre entre la solicitud de registro y la emisión del certificado depende del método de solicitud elegido por el Sujeto, o por el Suscriptor, y de si hay que recoger alguna información adicional o entregar físicamente el dispositivo.

4.2.4. NOTIFICACIÓN AL SUSCRIPTOR POR PARTE DE LA AC DE LA EMISIÓN DEL CERTIFICADO

En los certificados de entidad final emitidos por Camerfirma se envía una notificación por correo electrónico al Solicitante indicando la aprobación o denegación de la solicitud.

4.3. EMISIÓN DE CERTIFICADOS

4.3.1. ACCIONES DE LA AC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

4.3.1.1. CERTIFICADOS EMITIDOS EN SMARTCARD O TOKEN

La AR genera el par de claves criptográficas directamente en un dispositivo seguro de firma utilizando las aplicaciones que le proporciona la AC tras una autenticación segura.

La AR envía a la AC una solicitud de certificación de clave pública en formato PKCS#10. La solicitud se firma digitalmente con un certificado de firma cualificado especialmente autorizado. Tras confirmar que la firma del PKCS#10 es auténtica y que el sujeto está autorizado a presentar la solicitud, la AC genera un certificado cualificado que se envía a través de un canal seguro localizado dentro del dispositivo.

4.3.1.2. CERTIFICADOS EMITIDOS EN UN DISPOSITIVO DE FIRMA REMOTA (HSM)

El Sujeto o el Suscriptor se conectan a los servicios o aplicaciones de la AR.

La AR genera el par de claves criptográficas directamente en el HSM situado en las instalaciones del QTSP. A continuación, la AR envía a la AC una solicitud de certificación de clave pública a través de un canal seguro.

Tras confirmar que el sujeto tiene autorización para presentar la solicitud, la AC genera un certificado cualificado que se almacena en el HSM.

Los dispositivos cualificados cumplen la política de componente de servicio de aplicación de creación de firmas: itu-t(0) identified-organization(4) etsi(0) SERVICE CREATION-policies(19431) ades(2) policy-identifiers(1) eu-advancedx509(2) – [0.4.0.19431.2.1.2].

4.3.1.3. CERTIFICADOS EMITIDOS CON FINES DE PRUEBAS

A veces es necesario utilizar los certificados para realizar algunas pruebas en un entorno de producción.

En estos casos, antes de emitir el certificado es necesario proceder al registro de los datos. Este registro debe ser aprobado por el Responsable de Seguridad.

Los datos utilizados para el registro deben indicar claramente en el Asunto que se trata de un certificado de prueba y no de un certificado real.

Este procedimiento no puede utilizarse para pruebas de carga o pruebas cíclicas sobre registros y emisiones. Cuando la prueba específica ya no sea requerida, el certificado debe ser revocado de oficio.

4.3.2. NOTIFICACIÓN POR PARTE DE LA AC DE LA EMISIÓN DE UN CERTIFICADO AL SUSCRIPTOR

Si el certificado se emite en un dispositivo criptográfico, el Sujeto o el Suscriptor no necesita ser notificado de la emisión del certificado, ya que el certificado está incorporado al dispositivo que se le entrega.

En los demás casos, el Sujeto recibirá la notificación a través de la dirección de correo electrónico indicada en el momento del registro. Esta información también puede ser compartida con el Suscriptor.

4.3.3. ACTIVACIÓN

4.3.3.1. ACTIVACIÓN DEL DISPOSITIVO DE FIRMA (SMARTCARD O TOKEN)

Una vez recibido el dispositivo, el Sujeto, utilizando los códigos de activación que le han sido entregados confidencialmente y el software especial proporcionado por la AC, procede a activar el dispositivo eligiendo al mismo tiempo un PIN de firma, parámetro de seguridad confidencial cuyo secreto y protección recaen exclusivamente en el propio Sujeto.

4.3.3.2. ACTIVACIÓN DEL DISPOSITIVO DE FIRMA REMOTA (HSM)

Tras acceder a la página web de la AC utilizando los códigos de activación que se le han facilitado de forma confidencial, el Sujeto -o, en el caso de una persona jurídica, el Suscriptor- selecciona un PIN de firma, un parámetro de seguridad confidencial cuyo secreto y protección recaen exclusivamente en el propio Sujeto. Para confirmar el PIN, el Sujeto/Suscriptor introduce la contraseña de un solo uso recibida vía SMS, generada a través de un token o de la aplicación token asociada al certificado.

En algunos casos, el certificado puede emitirse ya activo y utilizable.

4.4. ACEPTACIÓN DE CERTIFICADOS

4.4.1. CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DEL CERTIFICADO

Una vez entregado o notificado el certificado, el usuario dispone de catorce días para comprobar que se ha emitido correctamente.

Si el certificado no se ha emitido correctamente por problemas técnicos, se revocará y se emitirá uno nuevo.

4.4.2. PUBLICACIÓN DEL CERTIFICADO POR LA AC

Una vez completado con éxito el procedimiento de certificación, el certificado se inscribirá en el Registro de Certificados correspondiente y la AC no lo hará público.

4.4.3. NOTIFICACIÓN DE LA EMISIÓN A TERCERAS PARTES

No estipulado.

4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO

4.5.1. USO DEL PAR DE CLAVES Y DEL CERTIFICADO DEL SUSCRIPTOR

Cualquier dispositivo de firma o herramienta de autenticación de firma remota debe ser custodiado por el Sujeto de forma segura. El Sujeto debe mantener la información de validación del uso de la clave privada separada del dispositivo, si está presente, o de las herramientas o códigos de autenticación. Además, debe garantizar la protección de la privacidad y la conservación del código de emergencia requerido para la revocación del certificado, mientras utiliza su certificado únicamente en la forma prescrita por esta DPC y por las leyes nacionales e internacionales aplicables.

El suscriptor no debe colocar ninguna firma electrónica utilizando claves privadas cuyo certificado haya sido revocado y debe abstenerse de utilizar certificados de firma emitidos por ACs revocadas.

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

CA	Key Usage	Extended Key Usage	Basic Constraints
CAMERFIRMA ROOT 2021	critical, cRLSign, keyCertSign	-	critical,CA:true
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical,CA:true
CERTIFICADO CUALIFICADO CORPORATIVO – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO CORPORATIVO – QCP-n-qscd en QSCD en la nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN – QCP-n-qscd en QSCD en la nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA CON PODERES GENERALES DE REPRESENTACIÓN – QCP-n-qscd en QSCD en la nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA TRÁMITES CON LAS AAPP – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA TRÁMITES CON LAS AAPP – QCP-n-qscd en QSCD en la nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA TRÁMITES CON LAS AAPP – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA TRÁMITES CON LAS AAPP – QCP-n-qscd en QSCD en la nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA APODERADOS – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE PERSONA JURÍDICA PARA APODERADOS – QCP-n-qscd en QSCD en nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA APODERADOS – QCP-n-qscd en QSCD SmartCard o Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

CA	Key Usage	Extended Key Usage	Basic Constraints
CERTIFICADO CUALIFICADO DE REPRESENTANTE DE ENTIDAD SIN PERSONALIDAD JURÍDICA PARA APODERADOS – QCP-n-qscd en QSCD en nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical,CA:false

Aunque el cifrado de datos con certificados es técnicamente posible, Camerfirma no se hace responsable de los daños resultantes en caso de que el titular no pueda recuperar la clave privada necesaria para descifrar la información.

4.5.2. USO DEL PAR DE CLAVES Y DEL CERTIFICADO DE LA PARTE QUE CONFÍA

Las Partes que Confían deben estar familiarizadas con el campo de uso del certificado tal y como se indica en la DPC y en el propio certificado. También deben confirmar la validez de un certificado antes de utilizar la clave pública contenida en él, asegurarse de que el certificado no ha sido revocado comprobando el servicio OCSP o CRL correspondiente y confirmar la existencia y el contenido de cualquier restricción de uso del par de claves, así como de cualquier poder de representación y cualificación profesional.

4.6. RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

N/A

4.7. RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

4.7.1. CIRCUNSTANCIAS PARA LA RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

La renovación con cambio de claves implica la emisión de un nuevo par de claves y de un certificado de firma utilizado para firmar documentos y transacciones.

Los certificados de la AC raíz y de las AC intermedias se emiten en un nuevo procedimiento a través de un proceso creado a tal efecto.

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

4.7.2. QUIEN PUEDE SOLICITAR LA RENOVACIÓN CON CAMBIO DE CLAVES

El Sujeto puede solicitar la renovación con cambio de claves de un certificado antes de su caducidad sólo si el certificado no ha sido revocado y si toda la información proporcionada en la emisión anterior sigue siendo válida. Un certificado no puede ser renovado con cambio de claves después de su fecha de caducidad, y en su lugar se debe solicitar un nuevo certificado.

4.7.3. PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN CON CAMBIO DE CLAVES

La renovación con cambio de claves de un certificado se realiza a través de un servicio específico prestado por la AC como parte de sus relaciones comerciales y contractuales con el Sujeto y con la AR.

4.7.4. NOTIFICACIÓN DE LA NUEVA EMISIÓN DE UN CERTIFICADO AL SUSCRIPTOR

La notificación de la emisión de un certificado renovado con cambio de claves se producirá como se estipula en la sección 4.3.2 de este documento.

4.7.5. CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DE UN CERTIFICADO RENOVADO CON CAMBIO DE CLAVES

Según lo establecido en la sección 4.4.1 de este documento.

4.7.6. PUBLICACIÓN DE UN CERTIFICADO RENOVADO CON CAMBIO DE CLAVES POR LA AC

Según lo establecido en la sección 4.4.2 de este documento.

4.7.7. NOTIFICACIÓN DE LA EMISIÓN DE UN CERTIFICADO RENOVADO CON CAMBIO DE CLAVES POR PARTE DE LA AC A OTRAS ENTIDADES

En algunos casos, los certificados de las entidades finales se envían al Organismo de Supervisión que regula las actividades de las ACs.

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

Los certificados de la AC raíz y de las AC intermedias se comunican al Organismo de Supervisión para su incorporación a la TSL.

4.8. MODIFICACIÓN DE CERTIFICADOS

N/A

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

Si un certificado es revocado, queda invalidado antes de su fecha de caducidad. Cualquier firma realizada después de la revocación queda invalidada. Los certificados revocados se marcan como tales en el servicio OCSP y en la CRL firmada por la AC. Esta lista se emite y se publica a intervalos determinados, véase la sección 4.9.7. En circunstancias especiales, la AC puede forzar la emisión de una CRL no planificada. La revocación se hace efectiva a partir del momento de la emisión de la lista, que se certifica con la fecha de registro del evento introducida en el Registro de Auditoría de la AC.

La información del estado de revocación se mantiene disponible en una AC (Raíz o Intermedia) durante 15 años después de la expiración del certificado de la AC Raíz mediante la emisión y el almacenamiento de la última CRL.

No se permite la suspensión de certificados.

Camerfirma mantiene la información sobre el estado de un certificado caducado a través de los servicios OCSP y/o CRL.

Debido a la diferente naturaleza de los servicios OCSP y CRL, en el caso de obtener diferentes respuestas para un certificado caducado, la respuesta dada por el OCSP se considerará como la respuesta válida.

Para Camerfirma, el servicio de consulta del estado de un certificado principal es el que ofrece OCSP.

Los certificados revocados no pueden ser utilizados bajo esta DPC.

4.9.1. CIRCUNSTANCIAS PARA LA REVOCACIÓN

Como regla general, un certificado será revocado cuando:

- Se modifica cualquiera de los datos que figuran en el certificado.
- Se detectan errores o datos incompletos en los datos presentados en la solicitud de certificado o se producen cambios en las circunstancias verificadas para la emisión del mismo.
- Falta de pago del certificado.
- Cese de la AC.

Debido a circunstancias que afectan a la seguridad de la clave o del certificado:

- La clave privada o las infraestructuras o sistemas pertenecientes a la AC que emitió el certificado están comprometidos, siempre que este incidente afecte a la fiabilidad de los certificados emitidos.
- La AC ha incumplido los requisitos de los procedimientos de gestión de certificados establecidos en esta DPC.
- La seguridad de la clave o del certificado perteneciente al Sujeto o al Responsable del certificado está comprometida o se sospecha que está comprometida.
- Existe un acceso o uso no autorizado por parte de terceros de la clave privada del Sujeto o del Responsable del certificado.
- Hay un mal uso del certificado por parte del Sujeto o del Responsable del certificado o no se mantiene segura la clave privada.

Debido a circunstancias que afectan a la seguridad del dispositivo criptográfico:

- La seguridad del dispositivo criptográfico está comprometida o se sospecha que está comprometida.

- Hay pérdida o inutilización por daños en el dispositivo criptográfico.
- Existe un acceso no autorizado de terceros a los datos de activación del Sujeto/Firmante o del responsable del certificado.
- Incumplimiento por parte del Suscriptor, el Sujeto o el Responsable de las normas de uso del dispositivo criptográfico establecidas en esta DPC o en los Términos y Condiciones.

Hay circunstancias que afectan al Sujeto, al Suscriptor, a la Entidad o al Responsable del certificado:

- La relación entre la AC y el suscriptor se da por terminada.
- Hay cambios o terminación de la relación legal subyacente o motivos para emitir el certificado al Sujeto.
- El solicitante incumple parte de los requisitos establecidos para solicitar el certificado.
- El Sujeto, la Entidad o el Responsable del certificado incumplen parte de sus obligaciones, responsabilidades y garantías establecidas en los Términos y Condiciones en esta DPC.
- La incapacidad repentina o la muerte del sujeto.
- Hay un cierre de la entidad relacionada con el Sujeto/Firmante del certificado.
- La autorización proporcionada por el Suscriptor al Sujeto o al Responsable del certificado ha cambiado o ha expirado, o la relación entre el Sujeto y el Responsable del certificado ha terminado.
- El Sujeto solicita la revocación del certificado de acuerdo con lo establecido en esta DPC.
- Resolución firme de la autoridad administrativa o judicial competente.
- El Sujeto indica que la solicitud de certificado original no fue autorizada y no concede la autorización con carácter retroactivo.
- En caso de que el Solicitante, el Sujeto o el Responsable soliciten a la AC la modificación o eliminación de sus datos personales de los registros de Camerfirma.

Otras circunstancias:

- Por la expedición de un certificado que no cumple los requisitos establecidos en esta DPC.
- Baja del servicio de la AC, de acuerdo con el apartado correspondiente de esta DPC, salvo que la gestión de los certificados emitidos haya sido transferida a otro Proveedor.

Para justificar la necesidad de la solicitud de revocación, hay que presentar los documentos necesarios a la AR o a la AC, según el motivo de la solicitud:

- Si la revocación es solicitada por el Sujeto o el Suscriptor, se deberá aportar una declaración firmada indicando el certificado a revocar y el motivo de esta solicitud e identificándose ante la AR.
- Si la revocación es solicitada por un tercero, deberá presentar autorización del Sujeto o del representante legal del titular del certificado de la Entidad. El tercero deberá indicar los motivos por los que solicita la revocación del certificado e identificarse ante la AR.
- Si la Entidad vinculada con el Sujeto solicita la revocación por la finalización de la relación con el mismo, deberá acreditarse esta circunstancia (revocación de poderes, finalización de contrato, etc.) y el Solicitante deberá identificarse ante la AR como autorizado para representar a la entidad.

4.9.2. QUIEN PUEDE SOLICITAR LA REVOCACIÓN

La solicitud de revocación del certificado se puede realizar por:

- El Suscriptor.
- El Sujeto/Titular.
- El Responsable.
- La Entidad. A través de un representante, cuando el Sujeto es una persona física vinculada con una organización.
- La AR o la AC.
- También contempla la posibilidad de que terceros o interesados puedan comunicar fraudes, usos indebidos, comportamientos inadecuados o datos erróneos, en cuyo caso, la AR o la AC podrán revocar el certificado tras comprobar la veracidad de las mencionadas causas de revocación.

La solicitud de revocación del certificado puede ser gestionada por:

- Los operadores autorizados de la AC o de la AR (Responsable de Revocación).

Adicionalmente, los operadores autorizados de la AC podrán tramitar la solicitud de revocación masiva de certificados por cese de actividad de la AC o de una AR.

En cualquier caso, en el momento de la revocación del certificado, se enviará una notificación por correo electrónico al Sujeto (certificado de firma electrónica) especificando la fecha y hora y el motivo de la revocación.

4.9.3. PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La revocación puede ser solicitada por los sujetos con derecho a ello mediante los siguientes procedimientos.

4.9.3.1. SOLICITUD DE REVOCACIÓN PRESENTADA POR EL SUJETO O POR EL RESPONSABLE

La solicitud de revocación es presentada por el Sujeto o por el Responsable utilizando los formularios disponibles en el sitio web de la AC. La solicitud debe ser firmada por el solicitante de la revocación y entregada a la AR o, alternativamente, enviada a la AC por carta, fax o correo electrónico acompañada de una copia de un documento de identidad válido. Además, la AC o la AR pueden poner a disposición métodos adicionales para presentar la solicitud de revocación, siempre que dichos métodos permitan una correcta identificación del Sujeto.

Una vez confirmada la autenticidad de la solicitud, la AC revoca el certificado y notifica la revocación al Sujeto con la mayor brevedad posible.

Si en el certificado al que se refiere la solicitud de revocación se incluye información de atributos, la revocación será notificada por la AC al Suscriptor con el que la AC haya suscrito un acuerdo específico. Si el nombre de la Entidad está incluido en el certificado al que se refiere la solicitud de revocación, la AC lo notificará a dicha Entidad.

Se podrán especificar métodos adicionales para solicitar la revocación por parte del Sujeto en eventuales acuerdos entre el Sujeto y la AC.

4.9.3.2. SOLICITUD DE REVOCACIÓN POR PARTE DE LA ENTIDAD O DEL SUSCRIPTOR

Para la solicitud de revocación del certificado del Sujeto presentada por la Entidad o el Suscriptor se aplican los mismos métodos que se aplican para la solicitud de revocación por el Sujeto o por el Responsable. La Entidad, a través de un representante, deberá especificar los datos del Sujeto facilitados a la AC en el momento de la emisión del certificado.

Una vez confirmada la autenticidad de la solicitud, la AC notifica al Suscriptor y al Sujeto por el medio de comunicación establecido al solicitar el certificado y procede a la revocación del certificado. Se pueden especificar métodos adicionales para las solicitudes de revocación en un acuerdo entre el Sujeto y la AC o la AR.

4.9.3.3. REVOCACIÓN DE LA AC/AR DE OFICIO

Cuando sea necesario, la AC/AR podrá revocar un certificado notificándolo previamente al Sujeto y especificando las circunstancias de la revocación, así como la fecha y hora de efecto.

Si en el certificado a revocar se incluye información de atributos, la revocación será notificada por la AC/AR al Suscriptor con el que la AC haya suscrito un acuerdo específico. Si el nombre de la Entidad está incluido en el certificado al que se refiere la solicitud de revocación, la AC notificará la revocación a dicha Entidad. La AC/AR comunicará la revocación también al Suscriptor.

4.9.4. PERIODO DE GRACIA DE REVOCACIÓN

Camerfirma podrá establecer periodos de gracia para la revocación en función de la naturaleza de cada caso.

4.9.5. PLAZO EN EL QUE LA AC DEBE TRAMITAR UNA SOLICITUD DE REVOCACIÓN

Camerfirma tramitará una solicitud de revocación de forma inmediata siguiendo el procedimiento descrito en el apartado 4.9.3.

El plazo máximo desde la recepción de una solicitud de revocación hasta su confirmación y tramitación será de 23 horas. Si la solicitud de revocación no puede confirmarse en este plazo, no se tramitará.

La AC tramitará inmediatamente las solicitudes de revocación que se confirmen y procesen. El tiempo máximo desde la tramitación hasta la publicación en los servicios de información de estado es de 1 hora.

El estado de revocación se publicará a más tardar 24 horas después de la recepción de la solicitud de revocación, de acuerdo con la normativa vigente.

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

Camerfirma en todo caso y conforme a esta CPS, puede revocar un certificado de forma unilateral e inmediata por motivos de seguridad, sin que el titular pueda reclamar ninguna indemnización por este hecho.

4.9.6. Requisitos de comprobación de para las Partes que Confían

Las partes que confían deben comprobar el estado de los certificados consultando las CRL o los servicios OCSP.

4.9.7. Frecuencia de emisión de CRL

La CRL emitida por la AC Raíz 'CAMERFIRMA ROOT 2021' tiene una frecuencia de emisión máxima de 365 días. Puede ser emitida antes de que acabe la primera hora después de que se haya revocado un certificado emitido por la CA Raíz.

La CRL de la AC intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' tiene una frecuencia de emisión de 1 hora.

4.9.8. Máxima latencia de CRL

La CRL de la CA Raíz 'CAMERFIRMA ROOT 2021' es publicada dentro de las siguientes 23 horas después de su emisión, antes del fin de validez de la CRL previa.

La CRL de la CA Intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' es publicada cuando es emitida, antes del fin de validez de la CRL previa.

4.9.9. Disponibilidad de comprobación on-line de la revocación

Todas las ACs descritas en esta DPC proporcionan un servicio OCSP de comprobación del estado de los certificados, hasta que la AC Raíz del certificado jerárquico caduque o hasta que la AC haya emitido una última CRL tras realizar una revocación masiva de todos los certificados vigentes.

4.9.10. Requisitos de la comprobación on-line de la revocación

Para comprobar la revocación en línea de un certificado con el servicio OCSP:

- Camerfirma pondrá a disposición de las partes que confían el servicio OCSP con la posibilidad de utilizar los métodos GET y POST.
- Camerfirma actualizará la información proporcionada a través del servicio OCSP de la AC Raíz 'CAMERFIRMA ROOT 2021' en las siguientes 24 horas tras la revocación de un certificado emitido por esta AC Raíz.
- Camerfirma actualizará en tiempo real la información proporcionada a través del servicio OCSP de la AC intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021'.

4.9.11. Otras formas de divulgación de información de revocación disponibles

N/A

4.9.12. Requisitos especiales de revocación por compromiso de las claves

Las Partes que detecten un compromiso de la clave pueden notificarlo enviando un correo electrónico a la dirección incidentes@camerfirma.com con el asunto "Notificación de compromiso de la clave", incluyendo la clave privada que ha sido comprometida.

4.9.13. Circunstancias de la suspensión

Las CA de esta DPC no suspenden certificados.

4.9.14. Quien puede solicitar una suspensión

No aplicable.

4.9.15. Procedimiento para la solicitud de suspensión

No aplicable.

4.9.16. LIMITES EN EL PERIODO DE SUSPENSIÓN
No aplicable.

4.10.SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1. CARACTERÍSTICAS OPERACIONALES
La información sobre el estado de los certificados está disponible a través de los servicios CRL y OCSP.

Camerfirma hará públicas las CRLs en las URLs que se incluyan en la extensión *CRL Distribution Point* de cada certificado.

Las CRLs emitidas por la CA intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021' incluyen certificados caducados.

Los certificados revocados que hayan caducado cuando la CA Raíz 'CAMERFIRMA ROOT 2021' emita la CRL no aparecerán en ella. En el caso de que esta CA Raíz se termine, Camerfirma incluirá cada certificado revocado, incluso los caducados, su motivo de revocación y el tiempo de revocación en la última CRL.

Camerfirma incluirá la URL de acceso a los servicios OCSP en la extensión denominada *Authority Information Access* en cada certificado de la cadena de certificación, excepto en los certificados de CA Raíz.

Camerfirma proporcionará información sobre el estado de los certificados caducados a través de los servicios OCSP después de su fecha de caducidad.

4.10.2. DISPONIBILIDAD DEL SERVICIO
Los servicios de estado de los certificados están disponibles las 24 horas del día, los siete días de la semana.

En caso de cualquier factor que no esté bajo el control de las AC, se hará lo posible para que este servicio de información esté disponible en 24 horas o menos.

4.10.3. CARACTERÍSTICAS OPCIONALES
No estipulado.

4.11.FINALIZACIÓN DE LA SUSCRIPCIÓN
La relación entre el Sujeto y/o el Suscriptor con las ACs se extingue cuando el certificado caduca o es revocado, salvo en casos especiales definidos por contrato.

4.12.CUSTODIA Y RECUPERACIÓN DE CLAVES
No estipulado.

5. CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES
Camerfirma como TSP ha implantado un sistema de seguridad de la información para su servicio de certificación digital. El sistema de seguridad se divide en tres niveles:

- Un nivel físico destinado a garantizar la seguridad de los entornos donde el TSP gestiona el servicio;
- Un nivel de procedimental de carácter estrictamente organizativo;
- Un nivel lógico que implica la disponibilidad de tecnología de hardware y software para hacer frente a los problemas y riesgos asociados con el tipo de servicio y la infraestructura utilizada.

Este sistema de seguridad está diseñado para evitar los riesgos derivados del mal funcionamiento de los sistemas, las redes y las aplicaciones, así como la intervención no autorizada o la modificación de los datos.

Puede solicitar un extracto de la política de seguridad de Camerfirma en https://www.camerfirma.com/contacto-soporte/ o en el teléfono +34 91 344 37 43.

5.1. CONTROLES DE SEGURIDAD FÍSICA
Las medidas aplicadas proporcionan una seguridad adecuada en:

- Características del emplazamiento y de la edificación;
- Sistemas anti-intrusión activos y pasivos;

- Control de acceso físico;
- Suministro de energía y aire acondicionado;
- Protección contra incendios;
- Protección contra inundaciones;
- Tipos de almacenamiento de los medios magnéticos;
- Sitios de almacenamiento de los medios magnéticos.

5.1.1. UBICACIÓN Y CONSTRUCCIÓN

Camerfirma utiliza tres instalaciones:

- La primera pertenece a Camerfirma y almacena las claves de la CA Raíz 'CAMERFIRMA ROOT 2021' utilizadas para la firma de certificados y CRLs y en ella se realizan las acciones necesarias relacionadas con los mismos.
- Camerfirma también utiliza las instalaciones de su empresa matriz InfoCert. En estas instalaciones se almacenan las claves de la CA intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021' utilizadas para la firma de certificados y CRLs, y se realizan las acciones necesarias relacionadas con las mismas.
- Camerfirma utiliza la nube de AWS para los servicios OCSP de toda la jerarquía.

Estas instalaciones se encuentran en:

- Las instalaciones de Camerfirma se encuentran en Ávila, España. Están construidas con materiales que garantizan la protección contra ataques mediante fuerza bruta y están situadas en una zona con bajo riesgo de desastres naturales y de rápido acceso.
  La sala donde se realizan las actividades criptográficas es una jaula de Faraday protegida contra la radiación externa, con doble suelo, sistema de detección y extinción de incendios, sistema antihumedad, doble sistema de refrigeración y doble sistema de alimentación eléctrica.
- El Centro de Datos de InfoCert está situado en Padua, Italia. El sitio de recuperación de desastres se encuentra en Módena y está conectado al Centro de Datos anterior mediante una conexión redundante dedicada en dos circuitos separados MPLS de 40 Gbit/s, cada uno de ellos actualizable a 100 Gbit/s.
  Dentro de ambos emplazamientos se han creado salas protegidas con varios sistemas de seguridad físicos y lógicos. Cada sala alberga los equipos informáticos que constituyen el núcleo de los servicios de certificación digital, sellado de tiempo y firma remota/automática.
- Para los servicios que necesitan continuidad de funcionamiento con valores de RTO/RPO cercanos a cero, algunos componentes de los servicios de las AC relativos a la publicación de las CRL y el OCSP se alojan en la nube de AWS, respectivamente, en la región de Frankfurt en Europa y en la región de Irlanda en Europa.
  AWS cuenta con certificaciones de conformidad según las normas ISO/IEC 27001:2013, 27017:2015, 27018:2019 e ISO/IEC 9001:2015.

5.1.2. ACCESO FÍSICO

El acceso a los Centros de Datos de Camerfirma, InfoCert y AWS se rige por los procedimientos de seguridad de Camerfirma, InfoCert y AWS.

5.1.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

El centro de datos de Camerfirma cuenta con estabilizadores de tensión y un sistema de alimentación doble con un generador.

Las salas en las que se almacenan los equipos informáticos disponen de sistemas de control de temperatura con unidades de aire acondicionado dobles.

Aunque no está certificado como tal, el sitio que alberga el centro de datos de InfoCert en Padua cumple los requisitos de un centro de datos Tier 3.

Las salas técnicas están equipadas con un sistema de alimentación eléctrica diseñado para evitar fallos, en especial de funcionamiento. Los sistemas de alimentación eléctrica cuentan con la tecnología más avanzada para aumentar la fiabilidad y garantizar la redundancia de las funciones más críticas que requieren los servicios prestados.

La infraestructura de suministro de energía incluye:

- Unidades de alimentación ininterrumpida, con acumuladores y basadas en corriente alterna (SAI);
- Disponibilidad de corriente alterna (220-380V AC);
- Armarios alimentados por redundancia con líneas protegidas dimensionadas para la absorción requerida;
- Servicio de generadores de emergencia;
- Conmutación y sincronización automática entre generadores, red y baterías (STS).

Cada armario técnico instalado en el Centro de Datos está alimentado por dos líneas de alimentación que aseguran la alta disponibilidad en caso de corte de una de las dos líneas disponibles.

El armario técnico se supervisa a distancia, con controles constantes del estado de las líneas de alimentación (encendido/apagado) y del consumo de energía (cada línea no debe superar el 50% de la carga).

La temperatura en el interior de la zona técnica se mantiene normalmente entre 20° y 27°, con un nivel de humedad relativa del 30% al 60%. Los sistemas están equipados con baterías de condensación con un sistema sellado de recogida y drenaje del condensado controlado por sensores anti-inundación. Todo el sistema de acondicionamiento está dedicado a los generadores de emergencia en caso de corte de energía. La capacidad de refrigeración de cada armario está garantizada con una carga máxima prevista de 10KW y un máximo de 15KW en dos armarios adosados.

5.1.4. EXPOSICIÓN AL AGUA

El Centro de Datos de Camerfirma se encuentra en una zona con bajo riesgo de inundación y no se encuentra en una planta baja. Las salas en las que se almacenan los equipos informáticos disponen de un sistema de detección de humedad.

La ubicación del centro no plantea riesgos para el medio ambiente derivados de la proximidad a instalaciones peligrosas. Durante el diseño del edificio, se tomaron las medidas oportunas para aislar los espacios potencialmente peligrosos, como los que contienen el grupo electrógeno y la instalación térmica. La sala de equipos se encuentra en la planta baja por encima del nivel de la calle.

5.1.5. PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

El Centro de Datos de Camerfirma cuenta con un sistema de detección y extinción automática de incendios. Los dispositivos criptográficos y los soportes que almacenan las claves de CA cuentan con un sistema de protección contra incendios específico y adicional al del resto de la instalación.

El Centro de Datos InfoCert cuenta con un sistema de detección de humos operado por una estación analógica NOTIFIER con sensores ópticos colocados en el entorno y en el falso techo y sensores de muestreo de aire instalados bajo el suelo y en los conductos de aire.

El sistema automático de detección de incendios está conectado a sistemas ecológicos de supresión de gases NAFS125 y PF23 y, en algunas salas, a sistemas de extinción por gas. En caso de activación simultánea de dos detectores en la misma zona, el gas se descarga en la zona afectada.

Cada compartimento de incendios cuenta con un sistema de extinción específico.

Además, hay medios de extinción portátiles que cumplen con las leyes y reglamentos aplicables.

Los conductos de aire primario conectados a las salas de equipos están provistos de persianas de extinción de incendios en el cruce de los compartimientos contra incendios. Estas compuertas son accionadas por el sistema automático de detección de incendios.

5.1.6. SISTEMA DE ALMACENAMIENTO

Cada dispositivo de almacenamiento desmontable sólo es accesible al personal autorizado.

Independientemente del dispositivo de almacenamiento, la información confidencial se guarda en armarios ignífugos o cerrados permanentemente y sólo se puede acceder a ella con autorización.

En cuanto a la plataforma de almacenamiento, la solución actual utiliza sistemas NetApp (FAS 8060) para la parte NAS. Para la parte SAN se ha implementado una infraestructura para el centro de llamadas basada en la tecnología Infinidat,

que incluye la caja Nº 2 InfiniBox de la generación F4000 y F6000. 2 InfiniBox de la generación F4000 y F6000; para la parte de la AC, la infraestructura se basa en la tecnología Pure Storage.

5.1.7. ELIMINACIÓN DE RESIDUOS

Camerfirma e InfoCert cuentan con la certificación ISO 14001 para la gestión medioambiental sostenible de su ciclo de producción, incluyendo la recogida diferenciada de residuos y la eliminación sostenible de los mismos. En cuanto al contenido de información de los residuos electrónicos, todos los soportes se borran de datos antes de su eliminación según los procedimientos aplicables o a través de empresas de tratamiento certificadas.

5.1.8. COPIA DE RESPALDO EXTERNA

Camerfirma guarda los documentos, dispositivos magnéticos y electrónicos en una caja fuerte, que está separada del centro de operaciones en un edificio externo seguro. Se requieren al menos dos personas expresamente autorizadas para acceder, almacenar o retirar dispositivos.

La copia de seguridad externa de InfoCert tiene lugar en el emplazamiento de recuperación de desastres a través de un dispositivo *EMC Data Domain 4200*, en el que el *Data Domain* primario del emplazamiento de Padua replica los datos de la copia de seguridad.

5.2. CONTROLES PROCEDIMENTALES

5.2.1. ROLES DE CONFIANZA

Los roles clave están cubiertos por personal que cuenta con la experiencia, la profesionalidad y los conocimientos técnicos/jurídicos necesarios, que se verifican constantemente mediante evaluaciones anuales.

Los roles de confianza de Camerfirma garantizan el reparto de funciones para distribuir el control y limitar el fraude interno y evitar que una sola persona controle todo el proceso de certificación de principio a fin, y con el mínimo privilegio concedido siempre que sea posible.

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

- Funciones asociadas al rol.
- Nivel de acceso.
- Control de operación.
- Formación y concienciación.
- Competencias requeridas.

Los roles de confianza de Camerfirma se ajustan a las normas ETSI EN 319 401 y ETSI EN 319 411-1:

- *Security Officers*: Responsabilidad general de la supervisión de la aplicación de las prácticas de seguridad.
- Administradores de Sistemas: Autorizados a instalar, configurar y mantener los sistemas de confianza del TSP para la gestión del servicio y, en su caso, la recuperación del sistema.
- Operadores de Sistemas: Responsables de operar los sistemas de confianza del TSP en el día a día. Autorizados a realizar copias de seguridad del sistema.
- Auditores de Sistemas: Autorizados a ver los archivos y registros de auditoría de los sistemas de confianza del TSP.
- Operadores de Registro: Autorizados para realizar la identificación de personas físicas y jurídicas y la emisión de certificados autorizados.
- Operadores de Revocación: Autorizados para realizar la revocación de certificados naturales y legales.

5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Camerfirma e InfoCert garantizan que al menos dos personas realizarán tareas clasificadas como sensibles, principalmente las relacionadas con las claves de las ACs.

5.2.3. IDENTIFICACIÓN AND AUTENTICACIÓN PARA CADA ROL

Cada persona sólo controla los activos necesarios para su rol, garantizando así que nadie acceda a recursos no asignados.

Dependiendo del activo, se accede a los recursos a través de un usuario/contraseña, certificados digitales, o llaves físicas, o SmartCard o Token y códigos de activación.

5.2.4. ROLES QUE REQUIEREN SEPARACIÓN DE TAREAS

El rol de confianza de *Security Officer* no puede ser ejercido por las mismas personas que ejercen cualquier otro rol de confianza.

5.3. CONTROLES DEL PERSONAL

5.3.1. CALIFICACIONES, EXPERIENCIA Y REQUISITOS DE AUTORIZACIÓN

El personal de Camerfirma que realice tareas clasificadas como de confianza debe tener al menos un año de antigüedad en el centro de trabajo y un contrato laboral indefinido.

El personal de Camerfirma está cualificado y ha sido formado en los procedimientos a los que ha sido asignado.

El personal de confianza no debe tener intereses personales que entren en conflicto con el desempeño de la función que se le encomienda.

Camerfirma se asegura de que el personal de registro u Operadores de AR sea de confianza y pertenezca a una Cámara de Comercio o al organismo delegado para realizar las labores de registro.

Los Operadores de AR deben haber realizado un curso de formación para las funciones de validación de solicitudes.

En general, Camerfirma retira las funciones de confianza de un empleado si descubre que ha cometido algún acto delictivo que pueda afectar al desempeño de sus funciones.

Camerfirma no asignará un puesto de confianza o de gestión a una persona que no sea apta para el puesto, especialmente por haber sido condenada por un delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se realizará previamente una investigación, en la medida en que lo permita la legislación aplicable, sobre los siguientes aspectos:

- Estudios, incluida la obtención de una titulación determinada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobando que el supuesto trabajo fue realmente realizado.
- Morosidad.

Camerfirma, tras la planificación anual de Recursos Humanos, el Responsable de la Función/Estructura Organizativa identifica las características y competencias del recurso a contratar (perfil del puesto). Posteriormente, junto con el Responsable de Selección de Personal, se inicia el proceso de búsqueda y selección.

5.3.2. PROCEDIMIENTOS DE COMPROBACIÓN DE ANTECEDENTES

Los procesos de Recursos Humanos de Camerfirma incluyen la realización de las investigaciones pertinentes antes de la contratación de cualquier persona.

Camerfirma nunca asigna funciones de confianza a personal que lleve menos de un año trabajando en la empresa.

En la solicitud de empleo se informa de la necesidad de someterse a una investigación previa y se advierte que la negativa a someterse a la misma supondrá el rechazo de la solicitud. Asimismo, se requiere el consentimiento incondicional del afectado para la investigación y para el tratamiento y protección de sus datos personales de acuerdo con la ley de Protección de Datos Personales.

Los candidatos seleccionados por Camerfirma participan en el proceso de selección mediante la realización de una primera entrevista cognitivo-motivacional con el Responsable de Selección de Personal y en una posterior entrevista técnica con el Responsable de Función/Estructura Organizativa, con el fin de comprobar las competencias declaradas por el candidato. Otras herramientas de verificación son los ejercicios y las pruebas.

5.3.3. REQUISITOS DE FORMACIÓN

El personal de Camerfirma que desempeñe funciones de confianza debe haber recibido formación de acuerdo con la PC. Existe un plan de formación que forma parte de los controles de la ISO/IEC 27001.

La formación incluye los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación pública.
- Versiones de los equipos y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tratamiento de incidentes y riesgos de seguridad.
- Continuidad de la actividad y procedimientos de emergencia.
- Procedimiento de gestión y seguridad relacionado con el tratamiento de datos personales.

Camerfirma impide que cualquier persona pueda afectar o alterar individualmente la seguridad global del sistema o realizar actividades no autorizadas, la gestión operativa del sistema está encomendada a diferentes responsables, cada uno con tareas separadas y bien definidas. El personal encargado del diseño y prestación de los servicios de certificación son empleados de Camerfirma seleccionados por su experiencia en el diseño, implantación y gestión de servicios informáticos y por su fiabilidad y confidencialidad. Periódicamente se programan sesiones de formación para que se familiaricen con las tareas asignadas. En particular, se imparten cursos de formación para proporcionar todas las habilidades necesarias (técnicas, organizativas y de procedimiento) para llevar a cabo las tareas asignadas antes de que el personal comience sus tareas operativas.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE LA ACTUALIZACIÓN DE LA FORMACIÓN

Camerfirma lleva a cabo los oportunos procesos de actualización para garantizar la correcta realización de las tareas de certificación, especialmente cuando se modifican sustancialmente.

A principios de cada año, se analizan las necesidades de formación de Camerfirma para definir los cursos de formación que se impartirán durante el año. El análisis se basa en los siguientes pasos:

- Reunión con la dirección para recopilar datos sobre los requisitos de formación necesarios para alcanzar los objetivos empresariales;
- Opiniones de los directores de área para identificar las necesidades de formación específicas de cada área;
- Transmisión de los datos recogidos a la dirección de la empresa para el cierre y la aprobación del plan de formación.

Una vez definido, el Plan de Formación de Camerfirma se comunica dentro de la empresa.

5.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

El horario de trabajo presencial o trabajo ágil (*smart working*) se distribuye en una franja horaria de 8:00 a 19:00 horas de lunes a viernes.

La cobertura del entorno de producción durante la noche y los días festivos se garantiza mediante un plan de rotación de guardia elaborado por el *Security Officer*. En función de las necesidades, las intervenciones pueden realizarse a distancia , intervención remota, o requerir el acceso a las instalaciones.

Siempre que se cumplan los requisitos técnicos y profesionales necesarios, Camerfirma e InfoCert garantizan el mayor número posible de trabajadores de guardia, dando prioridad a los empleados que lo soliciten.

5.3.6. SANCIONES POR ACCIONES NO AUTORIZADAS

Camerfirma tiene establecido un régimen sancionador interno, que se describe en su política de Recursos Humanos, para aplicar cuando un empleado realiza acciones no autorizadas, que incluye la posibilidad de despido.

Las sanciones de Camerfirma se imponen de acuerdo con el Estatuto de los Trabajadores y el convenio colectivo aplicable, Oficinas y Despachos.

5.3.7. REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL

Los empleados de Camerfirma contratados para realizar tareas de confianza deben firmar las cláusulas de confidencialidad y los requisitos operativos que utiliza Camerfirma. Cualquier acción que comprometa la seguridad de los procesos aceptados podría dar lugar a la rescisión del contrato del empleado, una vez evaluado.

En el caso de que la totalidad o parte de los servicios de certificación sean operados por un tercero, los controles y disposiciones realizadas en este apartado o en otras partes de la DPC son aplicados y ejecutados por el tercero que realiza las funciones operativas de los servicios de certificación, siendo la AC la responsable de la implementación real en todas las situaciones.

Estos aspectos se especifican en el instrumento legal utilizado para acordar la prestación de los servicios de certificación por parte de terceros distintos de Camerfirma, y los terceros deben estar obligados a cumplir los requisitos exigidos por Camerfirma.

Los requisitos de Camerfirma para el acceso de personal no empleado se rige por una política corporativa específica.

5.3.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Camerfirma pone a disposición de todo el personal la documentación que describe las tareas asignadas, haciendo hincapié en las normas de seguridad, la privacidad y la DPC.

Esta documentación se encuentra en un repositorio interno al que puede acceder cualquier empleado de Camerfirma; el repositorio contiene una lista de documentos que deben ser conocidos y cumplidos.

También se suministra la documentación que los empleados necesitan en cada momento para que puedan realizar sus tareas de forma competente.

En el momento de la contratación de Camerfirma, los empleados deberán aportar una copia de un documento de identidad válido, así como su número de identificación sanitaria vigente. Posteriormente, se les pedirá que completen y firmen un consentimiento escrito para el tratamiento de datos personales y un acuerdo de confidencialidad, y que revisen el Código Ético y la Política de Privacidad de Camerfirma.

5.4. PROCEDIMIENTOS DE REGISTRO DE EVENTOS

La gestión de la AC y los registros del ciclo de vida del certificado se recogen en el Registro de Auditoría, tal y como exige el Reglamento eIDAS.

5.4.1. TIPOS DE EVENTOS REGISTRADOS

Los registros archivados incluyen eventos de seguridad, eventos de arranque y apagado, caídas del sistema y fallos de hardware, actividad del firewall y del router, e intentos de acceso al sistema PKI.

Se conservan todos los datos y documentos utilizados durante la identificación y aceptación de las solicitudes de los Suscriptores, incluidas las copias de los documentos de identidad, los contratos, los extractos del registro comercial, etc.

También se registran los eventos de registro y ciclo de vida de los certificados. Entre ellos se encuentran la emisión de certificados y las solicitudes de renovación con cambio de clave, el registro de certificados, la generación, la distribución y la posible revocación.

Se registran todos los eventos relativos a la personalización del dispositivo de firma.

Se registran todos los accesos físicos a los lugares de alta seguridad donde se encuentran las máquinas de AC.

Se registran todos los accesos lógicos a las aplicaciones de la AC.

También se archivan todos los eventos de personalización del dispositivo de firma. Cada evento se guarda con su fecha y hora del sistema.

5.4.2. FRECUENCIA DE TRATAMIENTO DE REGISTROS DE AUDITORIA

La recogida de datos, la clasificación y el archivo en el sistema de conservación InfoCert se realizan mensualmente.

5.4.3. PERIODO DE RETENCIÓN PARA LOS REGISTROS DE AUDITORIA
El registro de auditoría es conservado por la AC durante 20 años.

5.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORIA
La protección del registro de auditoría está garantizada por el sistema de conservación de documentos electrónicos de InfoCert, acreditado por AgID de acuerdo con la legislación vigente.

5.4.5. PROCEDIMIENTOS DE COPIA DE RESPALDO DE LOS REGISTROS DE AUDITORIA
El sistema de conservación de documentos electrónicos de InfoCert aplica políticas y procedimientos de copia de seguridad que cumplen con los requisitos de su manual de seguridad.

5.4.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA
Los registros de eventos se recogen mediante procedimientos automáticos ad hoc y se archivan en el sistema de conservación de InfoCert según los métodos descritos en el manual de seguridad del sistema de conservación de InfoCert.

5.4.7. NOTIFICACIÓN AL SUJETO DE CAUSA DE EVENTO
No estipulado.

5.4.8. ANÁLISIS DE VULNERABILIDADES
InfoCert realiza periódicamente evaluaciones de vulnerabilidad del sistema y pruebas de penetración. En base a los resultados, se implementan todas las contramedidas necesarias para asegurar las aplicaciones.

5.5. ARCHIVO DE REGISTROS

5.5.1. TIPOS DE REGISTROS ARCHIVADOS
La AC o las AR almacenan la siguiente información que forma parte del ciclo de vida del certificado:

- Cualquier dato de auditoría de la AC y del módulo centralizado cualificado.
- Cualquier dato relacionado con los certificados, incluyendo la identificación, la autentificación y los acuerdos.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados y CRLs emitidos por las ACs.
- Todas las consultas y respuestas del servicio OCSP.

5.5.2. PERIODO DE RETENCIÓN DEL ARCHIVO
Las ACs conservan la documentación detallada en la sección 5.5.1 durante al menos 15 años después de la fecha de caducidad de cualquier certificado basado en dicha documentación.

5.5.3. PROTECCIÓN DEL ARCHIVO
La protección está garantizada por el sistema de conservación InfoCert, acreditado por AgID.

5.5.4. PROCEDIMIENTO DE COPIA DE RESPALDO DEL ARCHIVO
El sistema de conservación de documentos de InfoCert aplica políticas y procedimientos de copia de seguridad que cumplen con los requisitos de su manual de seguridad.

5.5.5. REQUISITOS DEL SISTEMA DE SELLADO DE TIEMPO DE LOS REGISTROS
Los registros archivados son fechados con una fuente fiable por los sistemas que los generan.

5.5.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA
Los registros se recogen mediante procedimientos automáticos específicos y se archivan en el sistema de conservación de documentos que se ajusta a InfoCert, según los métodos descritos en su manual de seguridad.

5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA
Todos los datos se almacenan en un sistema de conservación conforme en el que se realizan comprobaciones periódicas y precisas sobre el estado del sistema y la integridad de los datos. Los datos se muestran de acuerdo con las normas pertinentes.

5.6. CAMBIO DE CLAVE

Las claves de la AC, Raíz o Intermedia, se cambiarán antes de que el certificado de la AC caduque. La clave privada de la antigua AC sólo puede utilizarse para firmar CRLs mientras haya certificados activos emitidos por la antigua AC, es decir, firmados con la clave privada de la antigua AC. Se genera un nuevo certificado con la nueva clave pública de la AC y un CN, *common name*, diferente al del antiguo certificado de la AC.

Las claves y/o el certificado de una CA también se modifican cuando se produce un cambio en la tecnología criptográfica, es decir, en los algoritmos, el tamaño de las claves, etc., que lo requiera, o para cumplir con los requisitos de las normas y legislación aplicables.

Cada cambio de clave de la AC implica una modificación de esta DPC y se notifica al Ministerio de Asuntos Económicos y Transformación Digital.

5.7. RECUPERACIÓN EN CASO DE COMPROMISO DE CLAVES O DESASTRE

5.7.1. PROCEDIMIENTOS DE GESTIÓN DE INCIDENCIAS Y COMPROMISO DE CLAVES

Las ACs, Raíz e Intermedias, disponen de una descripción de sus procedimientos de gestión de incidentes en el sistema de gestión de seguridad de la información (SGSI) certificado por InfoCert y Camerfirma según la norma ISO 27000. Cualquier detección de incidentes es seguida inmediatamente por el análisis de los mismos, la definición de contramedidas correctivas y la elaboración de un informe por parte del responsable del servicio. De conformidad con el artículo 19 del Reglamento eIDAS, también se envía una copia al Organismo de Supervisión.

Mientras dure el incidente no se emitirán certificados digitales.

5.7.2. CORRUPCIÓN DE RECURSOS, APLICACIONES O DATOS

En caso de fallo del dispositivo de firma seguro HSM que contiene las claves de la AC, se utiliza en su lugar una clave de respaldo de certificación debidamente guardada y almacenada, y no es necesario revocar el certificado de la AC intermedia correspondiente ni desconfiar del certificado de la AC raíz correspondiente.

El software y los datos son objeto de copias de seguridad periódicas según los procedimientos internos de Camerfirma e InfoCert.

5.7.3. COMPROMISO DE LA CLAVE PRIVADA DE LA ENTIDAD

El compromiso de la clave privada de una AC, ya sea raíz o intermedia, se considera un evento especialmente crítico, ya que invalida los certificados emitidos y la información del estado de revocación firmada con esa clave. Por lo tanto, se presta especial atención a la protección de la clave privada de la AC y a todas las actividades de desarrollo y mantenimiento del sistema que puedan tener un impacto sobre ella.

Aunque se trata de un evento excepcional, InfoCert y Camerfirma han establecido un procedimiento detallado a seguir dentro de su SGSI certificado ISO 27000.

Una vez comprobado el compromiso de una clave privada de la AC, Camerfirma procederá con la mayor brevedad posible:

- informar al Organismo de Supervisión español en las próximas 24 horas,
- informar a las AR y a los clientes, ya sean Sujetos/Firmantes o Suscriptores, Partes que Confían y otras entidades con las que tiene acuerdos u otro tipo de relaciones, a través de la comunicación directa cuando sea posible, y a través de la comunicación en el sitio web de Camerfirma,
- informar que los certificados y la información relativa al estado de revocación que están firmados con esta clave privada de la AC no son válidos,
- revocar los certificados afectados,
- proporcionar de una forma fiable información sobre el estado de revocación de los certificados, firmados con una clave privada de una AC diferente,
- y proceder, si es necesario, a la emisión y acreditación de una nueva AC Intermedia o Raíz.

5.7.4. CONTINUIDAD DE NEGOCIO DESPUÉS DE UN DESASTRE

Camerfirma e InfoCert han adoptado los procedimientos necesarios para garantizar la continuidad de su actividad incluso en situaciones altamente críticas o de desastre.

5.8. CESE DE LA AC O DE UNA AR

Antes de que Camerfirma cese su actividad como TSP emisor de certificados bajo esta DPC:

- Proporcionará los fondos necesarios, a través de una partida presupuestaria y una póliza de seguro de responsabilidad civil, para completar los procesos de transferencia y/o cese.
- Deberá notificar al Organismo de Supervisión, con al menos tres meses de antelación, el cese de su actividad como TSP emisor de certificados y, en su caso, la Parte Confiable a la que transferirá cualquier obligación (véase más adelante).
- Notificará a todos los Suscriptores, Sujetos/Firmantes, Responsables, Partes que Confían y otras entidades con las que tenga acuerdos u otro tipo de relaciones, el cese de la actividad con al menos dos meses de antelación.
- Publicará en su página web o en cualquier otro medio accesible a los usuarios, la información pertinente relativa al cese de sus operaciones.
- Revocará cualquier autorización de entidades subcontratadas para actuar en nombre de cualquier AC de Camerfirma afectada por esta DPC en el procedimiento de emisión de certificados.
- Seguirá cumpliendo sus obligaciones relacionadas con el mantenimiento de la información de registro, la información sobre el estado de revocación y los archivos de registro de eventos, así como con el suministro de información sobre el estado de revocación, durante lo establecido en el período de tiempo indicado a los Suscriptores, Sujetos/Firmantes y Partes que Confían, o transferirá estas obligaciones a una parte de confianza.
- Comunicará al Organismo de Supervisión cualquier procedimiento concursal contra el TSP, así como cualquier otra circunstancia que impida la actividad de Camerfirma como TSP.
- Terminará cualquier AC de Camerfirma afectada por esta DPC (ver más adelante).

Todas estas actividades se incluirán de forma detallada en el Plan de Cese de Camerfirma.

Antes de que Camerfirma dé por terminada cualquier AC bajo esta DPC:

- En el caso de que el cese de la AC incluya su sustitución por una nueva AC o por otra ya existente, deberá notificarlo a todos los Suscriptores y Sujetos/Firmantes, ofreciéndoles emitir sus certificados con la otra AC.
- Revocará todos los certificados activos emitidos por esta AC.
- Emitirá y publicará una última CRL, incluyendo los certificados caducados revocados, y con el campo *nextUpdate* igual a "99991231235959Z".
- Si la AC es una AC intermedia, deberá revocar el certificado por la AC emisora correspondiente (normalmente una AC raíz).
- Destruirá la clave privada de la AC.
- Deberá notificar al Organismo de Supervisión y a otras entidades con las que tenga acuerdos u otro tipo de relaciones el cese de la AC y las acciones realizadas en dicho cese.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

Para poder prestar su servicio, la AC necesita generar un par de claves que permita firmar los certificados del Sujeto.

Dichas claves son generadas únicamente por el personal encargado específicamente de esta función. La generación de claves y firmas se realiza dentro de módulos criptográficos dedicados y certificados, tal y como exige la legislación vigente.

La protección de la clave privada de la AC está garantizada por el módulo criptográfico de generación y uso de claves. La clave privada sólo puede generarse si están presentes simultáneamente dos encargados de la generación de claves. La generación de la clave tiene lugar en presencia del responsable del servicio.

Las claves privadas de la AC se replican con el único fin de ser recuperadas tras la rotura del dispositivo de firma segura. La replicación tiene lugar mediante un procedimiento controlado por el que la clave y su contexto se duplican en múltiples dispositivos, tal como exigen los criterios de seguridad de los dispositivos HSM.

El módulo criptográfico utilizado para la generación de claves y la firma cumple con requisitos que garantizan:

- Cumplimiento del par de claves con los requisitos necesarios impuestos por los algoritmos de generación y verificación utilizados;
- Una probabilidad razonable de generación de pares potenciales;
- Identificación del Sujeto que activa el procedimiento de generación;
- Esa generación de la firma tiene lugar dentro del dispositivo para que la clave privada no pueda ser interceptada.

6.1.1.1. GENERACIÓN DEL PAR DE CLAVES DEL FIRMANTE

Las claves asimétricas se generan dentro de un dispositivo seguro de creación de firma (SSCD o QSCD, tipo HSM) proporcionado por Camerfirma utilizando las funcionalidades propias de los dispositivos.

Las claves tienen una longitud mínima de 2.048 bits.

6.1.1.2. HARDWARE/SOFTWARE DE GENERACIÓN DE CLAVES

Los Sujetos/Firmantes pueden crear sus propias claves en un dispositivo autorizado por Camerfirma. Ver apartado 6.1.1.1.

Las claves de las ACs Raíz e Intermedias utilizan un dispositivo criptográfico que cumple con las especificaciones FIPS-104-2 nivel 3 o EAL4+.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Las claves privadas están alojadas en un dispositivo criptográfico, que puede ser un SSCD o un QSCD.

Al entregar el dispositivo criptográfico al Sujeto, éste entra en plena posesión de la clave privada, que sólo puede emplear introduciendo un PIN que conoce sólo él.

Cuando el procedimiento de registro se realiza en presencia del Sujeto, el dispositivo se entrega en cuanto se generan las claves.

Si el proceso de registro no se realiza en presencia del Sujeto, el dispositivo se entrega según las vías previstas en el contrato, prestando atención a que el dispositivo y sus instrucciones de uso viajen por canales diferentes o se entreguen al Sujeto en dos momentos distintos. En algunos casos, el Sujeto puede disponer ya de los dispositivos, ya que han sido entregados con antelación según procedimientos seguros y previa identificación del Sujeto.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública se envía a Camerfirma para crear el certificado cuando el circuito lo precise. Se entrega en formato estándar PKCS#10.

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LAS PARTES QUE CONFÍAN

Ver Sección 2.2.3.

6.1.5. TAMAÑO DE CLAVES

El par de claves asimétricas de los certificados se genera en los dispositivos de hardware criptográficos mencionados anteriormente.

Las claves de la AC Raíz y de las AC Intermedias pueden ser:

- Claves asimétricas RSA con una longitud de no menos de 4.096 bits;
- Claves asimétricas EC en una de las curvas elípticas proporcionadas por el documento ETSI TS 119 312 - *Cryptographic Suites* con una longitud no inferior a 256 bits.

Las claves del certificado de entidad final pueden ser:

- Claves asimétricas RSA con una longitud de no menos de 2.048 bits;
- Claves asimétricas EC en una de las curvas elípticas proporcionadas por el documento ETSI TS 119 312 - *Cryptographic Suites* con una longitud no inferior a 256 bits.

6.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y COMPROBACIÓN DE LA CALIDAD DE LOS PARÁMETROS

Los dispositivos se certifican de acuerdo con elevados estándares de seguridad (véase la sección 6.2.1) y garantizan que la clave pública es correcta y aleatoria. Antes de emitir un certificado, la AC verifica que la clave pública no se había utilizado previamente.

6.1.7. PROPÓSITOS DE USO DE LA CLAVE (CAMPO *KEY USAGE* DE X.509 V3)

Los propósitos de uso de las claves se determinan mediante la extensión *KeyUsage*, definida en el estándar X509. Para los certificados cubiertos por esta DPC, los usos permitidos son "*contentCommitment*", "*digitalSignature*" y/o "*keyEncipherment*".

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1. CONTROLES Y ESTÁNDARES DE MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos utilizados por Camerfirma para las claves de certificación (AC) y el respondedor OCSP están certificados FIPS 140 Nivel 3 y *Common Criteria* (CC) *Information Technology Evaluation Assurance Level* (EAL) EAL 4+ Tipo 3 (EAL 4 Ampliado por AVA_VLA.4 y AVA_MSU.3) en Europa.

Los dispositivos QSCD SmartCard o Token utilizados por Camerfirma están validados CC EAL 4+ *Type* 3 (EAL 4 Ampliado por AVA_VLA.4 and AVA_MSU.3), o EAL5 Ampliado por ALC_DVS.2, AVA_VAN.5.

Los dispositivos QSCD en Nube cuentan con la certificación FIPS 140 Nivel 3 y/o CC EAL 4+.

Camerfirma comprobará la conformidad de los dispositivos QSCD SmartCard o Token y dispositivos QSCD Cloud utilizados con el Reglamento eIDAS, bien con la última lista de estos dispositivos publicada por la UE o bien mediante notificación del Organismo de Supervisión. Si Camerfirma detecta en estas comprobaciones que alguno de estos dispositivos deja de tener la calificación de QSCD, Camerfirma revocará todos los certificados activos en los que la clave privada se encuentre en dichos dispositivos.

6.2.2. CONTROL MULTI-PERSONAL (N DE ENTRE M) DE LA CLAVE PRIVADA

El acceso a los dispositivos que contienen las claves de certificación sólo puede realizarse cuando dos personas se autentifican de forma simultánea.

6.2.3. DEPÓSITO DE CLAVE PRIVADA

No estipulado.

6.2.4. COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

La copia de seguridad de las claves privadas de las ACs está contenida en una caja fuerte cuyo código de acceso únicamente se asigna al personal que no tiene acceso a los dispositivos HSM. Por lo tanto, la restauración de claves requiere que tanto el personal encargado del dispositivo como los empleados que tienen acceso a la caja fuerte estén presentes al mismo tiempo.

6.2.5. ARCHIVO DE LA CLAVE PRIVADA

La copia de seguridad de las claves privadas de las ACs está contenida en una caja fuerte cuyo código de acceso únicamente se asigna al personal que no tiene acceso a los dispositivos HSM. Por lo tanto, la restauración de claves requiere que tanto el personal encargado del dispositivo como los empleados que tienen acceso a la caja fuerte estén presentes al mismo tiempo.

6.2.6. TRANSFERENCIA DE CLAVES PRIVADAS DESDE O A UN MÓDULO CRIPTOGRÁFICO

No estipulado.

6.2.7. ALMACENAMIENTO DE CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Las claves privadas de certificación se generan y almacenan en una zona segura del dispositivo criptográfico, gestionada por la entidad certificadora, que impide su exportación. Además, si se produce un intento de forzar la protección, el sistema operativo del dispositivo lo bloquea o se hace ilegible.

6.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves privadas de certificación son activadas por el software de la AC mediante doble control, es decir, por dos empleados con funciones específicas y en presencia del responsable del servicio.

El Sujeto o el Suscriptor que actúe como representante legal de una persona jurídica es responsable de proteger su clave privada con una contraseña segura para evitar su uso no autorizado. Para activar la clave privada, el Sujeto debe autenticarse.

6.2.9. MÉTODO DE DESACTIVAR LA CLAVE PRIVADA

No estipulado.

6.2.10. MÉTODO DE DESTRUIR LA CLAVE PRIVADA

El personal de Camerfirma e InfoCert encargado de esta función se ocupa de la destrucción de las claves privadas de las AC cuando los certificados caducan o son revocados, según los procedimientos de seguridad previstos en las políticas de seguridad y las especificaciones del fabricante del dispositivo.

6.2.11. CALIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

No estipulado.

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

No estipulado.

6.3.2. PERIODO DE USO PARA LAS CLAVES PÚBLICAS Y PRIVADAS

El periodo de validez del certificado se determinará en función de:

- El estado de la tecnología;
- El estado del arte de la tecnología criptográfica;
- El uso destinado al certificado.

Actualmente, los certificados de las AC tienen una validez máxima de 24 años. Los certificados expedidos a personas físicas o jurídicas tienen una validez máxima de 39 meses.

6.4. DATOS DE ACTIVACIÓN

Ver las secciones 4.3.3 y 6.3.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Camerfirma e InfoCert utiliza sistemas fiables para la prestación de los servicios de certificación. Camerfirma e InfoCert han realizado controles y auditorías informáticas para gestionar sus activos informáticos con el nivel de seguridad requerido para la gestión de los sistemas de certificación digital.

En relación con la seguridad de la información, se sigue el modelo de certificación sobre sistemas de gestión de la información ISO 270001.

6.5.1. REQUERIMIENTOS TÉCNICOS DE SEGURIDAD INFORMÁTICA ESPECÍFICOS

El sistema operativo de los ordenadores utilizados en las actividades de certificación que participan en la generación de claves, la generación de certificados y la gestión del registro de certificados están reforzados, es decir, están configurados para minimizar el impacto de cualquier vulnerabilidad mediante la eliminación de las características que no son necesarias para el funcionamiento y la gestión de la AC.

Los administradores de sistemas encargados de ello, de acuerdo con la normativa aplicable, accederán al sistema mediante una aplicación de *root on demand*, que permite utilizar los privilegios de usuario *root* sólo tras una autentificación individual. Cada acceso es rastreado, registrado y almacenado durante 12 meses.

6.5.2. VALORACIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad informática figura en un primer análisis de riesgos, de manera que las medidas de seguridad aplicadas responden a la probabilidad de que un grupo de amenazas vulnere la seguridad y a su impacto.

6.6. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Los certificados almacenan las claves del Firmante en un dispositivo cualificado de creación de firma (Hardware). El dispositivo de hardware es una SmartCard o Token criptográfico certificado como dispositivo cualificado de creación de firma de acuerdo con el Apéndice II de eIDAS.

Respecto a los dispositivos físicos:

- Los dispositivos de hardware son preparados y sellados por el proveedor independiente.
- El proveedor externo envía el dispositivo a la AR para que lo entregue al Firmante.
- El Firmante o la AR utiliza el dispositivo para generar el par de claves y transmitir la clave pública a la AC.
- La AC envía un certificado de clave pública al Firmante o a la AR, que se incorpora al dispositivo.
- El dispositivo se puede reutilizar y puede almacenar varios pares de claves de forma segura.
- El dispositivo es propiedad del Sujeto/Firmante.

Con respecto a los dispositivos utilizados en la gestión de QSCD en nube: El dispositivo que almacena estas claves tiene la certificación FIPS-104-2 nivel 3 o EAL4+ y está autorizado por el Organismo de Supervisión para los servicios catalogados como *QSCDManagedOnBehalf*.

6.6.1. CONTROLES DE DESARROLLO DEL SISTEMA

Camerfirma dispone de un procedimiento para controlar los cambios de versión del sistema operativo y de las aplicaciones que impliquen actualizaciones de las funciones de seguridad o para resolver cualquier vulnerabilidad detectada.

6.6.2. CONTROLES DE GESTIÓN DE LA SEGURIDAD

6.6.2.1. GESTIÓN DE LA SEGURIDAD

Camerfirma organiza las actividades de formación y sensibilización necesarias para los empleados en el ámbito de la seguridad. Los materiales de formación utilizados y las fichas de los procesos se actualizan una vez aprobados por un grupo de gestión de la seguridad.

Para ello se establece un plan de formación anual.

Camerfirma establece en los contratos las medidas de seguridad equivalentes para cualquier proveedor externo que participe en los trabajos de certificación.

6.6.2.2. CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN Y BIENES

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

La política de seguridad de Camerfirma describe los procedimientos de gestión de la información, clasificándolos según el nivel de confidencialidad.

Los documentos se clasifican en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.6.2.3. OPERACIONES DE GESTIÓN

Camerfirma ha establecido un procedimiento de gestión y respuesta a incidentes a través de un sistema de alertas e informes periódicos. El documento de seguridad de Camerfirma describe detalladamente el proceso de gestión de incidentes.

Camerfirma registra los procedimientos completos relativos a las funciones y responsabilidades del personal involucrado en el control y gestión de los elementos del proceso de certificación.

Todos los dispositivos se procesan de forma segura de acuerdo con los requisitos de clasificación de la información. Los dispositivos que contienen datos confidenciales se destruyen de forma segura si ya no son necesarios.

Camerfirma dispone de un procedimiento de refuerzo de sistemas en el que se definen los procesos para la instalación segura de los equipos. Las medidas descritas incluyen la anulación de servicios y accesos no utilizados por los servicios instalados.

El departamento de Sistemas de Camerfirma mantiene un registro de la capacidad de los equipos. Junto con la aplicación de control de recursos, se puede redimensionar cada sistema.

Camerfirma ha establecido un procedimiento para el seguimiento de las incidencias y su resolución, que incluye el registro de las respuestas y la evaluación económica de la solución de la incidencia.

Camerfirma define las actividades asignadas a personas con un rol de confianza distintas a las responsables de realizar las actividades diarias que no son confidenciales.

6.6.2.4. GESTIÓN DEL SISTEMA DE ACCESO

Camerfirma hace todo lo posible para que el acceso esté limitado al personal autorizado. En particular:

- Hay controles basados en cortafuegos, antivirus e IDS con alta disponibilidad.
- Los datos confidenciales se protegen mediante métodos criptográficos o estrictos controles de acceso de identificación.
- Camerfirma ha establecido un procedimiento documentado para tramitar las altas y bajas de usuarios y una política de acceso detallada en su política de seguridad.
- Camerfirma ha implementado procedimientos para garantizar que las tareas se realizan de acuerdo con la política de roles.
- A cada persona se le asigna un rol para llevar a cabo los procedimientos de certificación.
- Los empleados de Camerfirma son responsables de sus acciones según el acuerdo de confidencialidad firmado con la empresa.
- Creación del certificado: La autenticación para el proceso de emisión se realiza mediante un sistema de m de n operadores para activar la clave privada de la AC.
- Gestión de la revocación: La revocación se realiza a través de la autenticación estricta basada en SmartCard o Token de las solicitudes de un administrador autorizado. Los sistemas de registro de auditoría generan pruebas que garantizan el no repudio de la acción realizada por el administrador de la AC.
- Estado de revocación: La aplicación de estado de revocación incluye un control de acceso basado en la autenticación a través de certificados para evitar los intentos de manipulación de la información de estado de revocación.

6.6.2.5. GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

Camerfirma inspecciona el material entregado para asegurarse que el hardware criptográfico utilizado para firmar los certificados no es manipulado durante el transporte.

El hardware criptográfico se transporta con medios diseñados para evitar cualquier manipulación.

Camerfirma registra toda la información importante que contiene el dispositivo para incorporarla al catálogo de activos.

Se requieren al menos dos empleados de confianza para poder utilizar el hardware criptográfico para la firma de certificados.

Camerfirma realiza pruebas periódicas para garantizar el perfecto funcionamiento del dispositivo.

El dispositivo de hardware criptográfico sólo es manejado por personal de confianza.

La clave privada de firma de la AC almacenada en el hardware criptográfico será eliminada una vez retirado el dispositivo.

La configuración del sistema de la AC y sus modificaciones y actualizaciones quedan registradas y controladas.

Camerfirma ha establecido un contrato de mantenimiento del dispositivo. Las modificaciones o actualizaciones son autorizadas por el responsable de seguridad y registradas en los registros de trabajo correspondientes. Estas configuraciones son realizadas por al menos dos empleados de confianza.

6.6.3. EVALUACIÓN DE LA SEGURIDAD DEL CICLO DE VIDA
No estipulado.

6.7. CONTROLES DE SEGURIDAD DE RED
Para su servicio de certificación, Camerfirma e InfoCert han diseñado una infraestructura de seguridad de red basada en mecanismos de cortafuegos y en el protocolo SSL para proporcionar un canal seguro entre las AR y el sistema de certificación, y entre el sistema de certificación y los administradores/operadores.

Los sistemas y redes de Camerfirma e InfoCert se conectan a Internet de forma controlada mediante sistemas de cortafuegos que permiten dividir la conexión en zonas progresivamente más seguras: Redes de Internet, DMZ (Zona Desmilitarizada) o Redes Perimetrales, y Redes Internas. Todo el tráfico que fluye entre las áreas está sujeto a la aceptación del cortafuegos, en base a un conjunto de reglas establecidas. Las reglas del cortafuegos se diseñan basándose en los principios de "denegación por defecto" (lo que no está expresamente permitido se prohíbe por defecto, o las reglas sólo permitirán lo estrictamente necesario para que la aplicación funcione correctamente) y de "defensa en profundidad" (se disponen capas de defensa crecientes, primero a nivel de red, a través de sucesivas barreras de cortafuegos, y finalmente a nivel de sistema a través de *hardening*).

6.8. FUENTE DE TIEMPO
Para implementar una referencia temporal del sistema precisa, exacta y fiable, utilizada por todos los sistemas implicados en la generación de certificados y CRLs emitidos por las ACs intermedias, la solución operativa se basa en dispositivos físicos que actúan como servidores NTP sincronizados a través de las señales proporcionadas por los sistemas de satélites GPS y GLONASS. Los servidores NTP también pueden utilizar los servidores NTP del INRIM como referencia temporal adicional. Toda la arquitectura se encuentra en alta disponibilidad.

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1. PERFILES DE CERTIFICADOS
Los perfiles de los certificados cumplen con el IETF RFC 5280.

Todos los certificados cualificados emitidos de acuerdo con esta política cumplen la norma X.509 versión 3 de la ITU, así como la IETF RFC 3739 y los diferentes perfiles descritos en la ETSI EN 319 412.

Camerfirma publica el detalle de los campos básicos del certificado y las extensiones del certificado de los tipos de certificados emitidos en las jerarquías descritas en esta DPC en https://policy21.camerfirma.com.

7.1.1. NÚMERO DE VERSIÓN
Camerfirma emite certificados X.509 Versión 3.

7.1.2. EXTENSIONES DE LOS CERTIFICADOS
Ver la Sección 7.1.

7.1.3. IDENTIFICADORES DE OBJETO DE LOS ALGORITMOS
El identificador del objeto del algoritmo de firma podría ser:

- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption
- 1.2.840.113549.1.1.12 - sha384WithRSAEncryption
- 1.2.840.113549.1.1.13 - sha512WithRSAEncryption

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

7.1.4. FORMATO DE NOMBRES
Los certificados deben contener la información que se requiere para su uso, según lo establecido en la correspondiente política de autenticación, firma digital, cifrado o evidencia digital.

En general, los certificados para uso en el sector público deben contener la identidad de la persona que los obtiene, preferentemente en los campos Nombre del Sujeto o Nombre Alternativo del Sujeto, incluyendo los siguientes datos:

- El nombre completo de la persona Firmante, titular del certificado o representado, en campos separados, o indicando el algoritmo que permite la separación de forma automática.
- Nombre de la persona jurídica, cuando proceda.
- Números de los documentos de identificación correspondientes, de acuerdo con la legislación aplicable a la persona Firmante, titular del certificado o representada, ya sea persona física o jurídica.

La semántica exacta de los nombres se describe en las fichas de perfil. Véase la sección 7.1 para obtener información sobre las fichas de perfil.

7.1.5. RESTRICCIONES DE LOS NOMBRES
No estipulado.

7.1.6. IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN
Todos los certificados tienen un identificador de política que parte de la base 1.3.6.1.4.1.17326.

7.1.7. USO DE LA EXTENSIÓN *POLICY CONSTRAINTS*
No estipulado.

7.1.8. SINTAXIS Y SEMÁNTICA DE LOS CALIFICADORES DE POLÍTICA
No estipulado.

7.1.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA *CERTIFICATE POLICY*
La extensión "*Certificate Policy*" identifica la política que define las prácticas que Camerfirma asocia explícitamente al certificado. La extensión puede contener un calificador de la política. Ver apartado 7.1.6.

7.2. PERFIL DE CRL
Las CRLs de Camerfirma cumplen con el IETF RFC 5280.

Las CRLs están firmadas por la AC que emitió los certificados.

La CRL de la AC Raíz 'CAMERFIRMA ROOT 2021' tiene una validez de 365 días.

Las CRLs de la AC intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021' tienen una validez de 24 horas.

7.2.1. NÚMERO DE VERSIÓN
Las CRLs emitidas por Camerfirma son versión 2.

7.2.2. CRL Y EXTENSIONES
Todas las CRLs emitidas por Camerfirma incluyen las siguientes extensiones:
- *CRL Number* (OID 2.5.29.20), como se define en el IETF RFC 5280.
- *Authority Key Identifier* (OID 2.5.29.35), como se define en el IETF RFC 5280 e incluyendo únicamente el campo *keyIdentifier*.

Todas las CRLs emitidas por la AC Intermedia 'AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021' incluyen las siguientes extensiones de CRL:
- *ExpiredCertsOnCRL* (OID 2.5.29.60), como se define en ISO/IEC 9594-8/*Recommendation* ITU-T X.509 y se ajusta al valor de fecha y hora "notBefore" del certificado de la AC.
- *Issuing Distribution Point* (OID 2.5.29) como se define en IETF RFC 5280.

Las entradas de las CRLs incluyen las siguiente extensión:
- *Reason Code* (OID 2.5.29.21), como se define en IETF RFC 5280.

7.3. PERFIL DE OCSP
El perfil de las respuestas OCSP cumple con el IETF RFC 6960.

Camerfirma incluirá el motivo de la revocación en las respuestas OCSP dentro de la información de cada certificado revocado.

El perfil de los certificados de respondedor OCSP cumple con la sección 7.1 de la DPC.

7.3.1. NÚMERO DE VERSIÓN
Conforme al IETF RFC 6960.

7.3.2. EXTENSIONES OCSP
Las ACs Raíces y las ACs Intermedias de Camerfirma incluyen en las respuestas OCSP las siguientes extensiones:

- *Nonce* (OID 1.3.6.1.5.5.7.48.1.2), como se define en el RFC 6960 del IETF y como extensión no crítica.
- *Archive CutOff* (OID 1.3.6.1.5.5.7.48.1.6), tal y como se define en el RFC 6960 del IETF, ajustado al valor de fecha y hora "*notBefore*" del certificado de la AC y como extensión no crítica.
- *Extended Revoked Definition* (OID 1.3.6.1.5.5.7.48.1.9), como se define en el RFC 6960 del IETF y como extensión no crítica.

8. AUDITORÍAS DE CONFORMIDAD

8.1. FRECUENCIA DE LAS AUDITORÍAS
Camerfirma realizará periódicamente las auditorías necesarias. Esta periodicidad es fundamentalmente anual.

8.2. IDENTIFICACIÓN Y CALIFICACIONES DEL AUDITOR
Las auditorías son llevadas a cabo por empresas externas independientes ampliamente reconocidas en materia de seguridad informática, seguridad de los sistemas de información y auditorías de cumplimiento para las ACs.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD
Las empresas auditoras contratadas son empresas independientes y de reconocido prestigio, con departamentos de auditoría informática especializados en la gestión de certificados digitales y servicios de confianza, lo que descarta cualquier conflicto de intereses que pueda afectar a sus actividades en relación con las ACs.

No existe ninguna asociación financiera u organizativa entre las empresas auditoras y las ACs.

8.4. PUNTOS CUBIERTOS POR LA AUDITORÍA
En términos generales, las auditorías verifican:

- Que Camerfirma tiene un sistema que garantiza la calidad del servicio.
- Que Camerfirma cumple con los requisitos de las PCs que regulan la emisión de los diferentes certificados digitales.
- Que la DPC se ajusta a las disposiciones de las PCs, con el consentimiento de la AP y con los requisitos de la legislación vigente.
- Que la AC gestione adecuadamente la seguridad de sus sistemas de información.

Los elementos auditados son:

- Las ACs, las ARs y los servicios de validación.
- Los sistemas de información.
- Los centros de datos.
- Documentación necesaria para cada tipo de certificado.
- Verificación de que los operadores de las RAs conocen el DPC de las ACs.

8.5. MEDIDAS ADOPTADAS A RAÍZ DE LAS DEFICIENCIAS
Una vez recibido el informe de cumplimiento de la auditoría, Camerfirma analiza las deficiencias encontradas con la entidad que ha realizado la auditoría y desarrolla e implementa un plan correctivo para solventar dichas deficiencias.

Si la entidad auditada no es capaz de desarrollar y/o implementar el plan en el plazo requerido, o si las deficiencias suponen una amenaza inmediata para la seguridad o la integridad del sistema, se notificará inmediatamente a la AP, que podrá tomar las siguientes medidas:

- Cese temporal de las operaciones.
- Revocar el/los certificado/s pertinente/s y restaurar la infraestructura.

- Cese del servicio de la Entidad.
- Otras medidas complementarias que sean pertinentes.

8.6. COMUNICACIÓN DE RESULTADOS

La comunicación de los resultados será realizada por los auditores que han realizado la auditoría al responsable de seguridad y de cumplimiento normativo. Se realiza en un acto con la presencia de la dirección de la entidad.

9. ASPECTOS LEGALES Y OTROS ASUNTOS

9.1. TARIFAS

9.1.1. TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

Los precios de los servicios de certificación o cualquier otro servicio relacionado están publicados y son actualizados en la web de Camerfirma.

El precio determinado de cada tipo de certificado se publica, excepto los que son objeto de negociación previa.

9.1.2. TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso al registro público de certificados emitidos es gratuito.

9.1.3. TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS O LOS CERTIFICADOS REVOCADOS.

Camerfirma provee de forma gratuita el acceso a la información relativa al estado de los certificados a través de la CRL o del servicio OCSP.

9.1.4. TARIFAS DE OTROS SERVICIOS

Se puede acceder gratuitamente a esta DPC en el sitio web de Camerfirma https://policy21.camerfirma.com.

9.1.5. POLÍTICA DE REINTEGROS

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

La correcta emisión del certificado digital, sea en el soporte que sea, supone el inicio de la ejecución del contrato, con lo que, según la Ley General para la Defensa de los Consumidores y Usuarios (RDL 1/2007) en tales casos, el Sujeto/Titular pierde su derecho de desistimiento.

9.2. RESPONSABILIDAD FINANCIERA

9.2.1. COBERTURA DEL SEGURO

Camerfirma, en su calidad de PSC, dispone de una póliza de seguro de responsabilidad civil que cubre la responsabilidad de pago de indemnizaciones por daños y perjuicios causados a los usuarios de sus servicios: Sujeto/Firmante y Parte que Confía y terceros, por un importe mínimo de 1.500.000 € más 500.000 € por cada servicio cualificado eIDAS.

9.2.2. OTROS ACTIVOS

No estipulado.

9.2.3. SEGURO O COBERTURA DE GARANTÍA PARA ENTIDADES FINALES

Ver sección 9.2.1.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN DEL NEGOCIO

9.3.1. INFORMACIÓN CONSIDERADA COMO CONFIDENCIAL

Camerfirma considera confidencial cualquier información no clasificada como pública. La información declarada confidencial no se divulga sin el consentimiento explícito y por escrito de la entidad u organización que clasificó esta información como confidencial, salvo que lo establezca la ley.

Camerfirma ha establecido una política de tratamiento de la información y de los archivos de acuerdo con su confidencialidad, que cualquier persona que acceda a información confidencial debe firmar.

Camerfirma cumple con la legislación vigente en materia de protección de datos personales:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

9.3.2. INFORMACIÓN CONSIDERADA COMO NO CONFIDENCIAL

Camerfirma considera que la siguiente información no es confidencial:

- El contenido de esta DPC y CP.
- La información incluida en los certificados, CRLs y respuestas OCSP.

9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Camerfirma es responsable de la protección de la información confidencial generada o comunicada durante todas las operaciones. Las AR son responsables de la protección de la información confidencial que haya sido generada o almacenada por sus propios medios.

En el caso de las entidades finales, el Sujeto o el Responsable del certificado son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesaria para acceder o utilizar la clave privada.

9.4. PRIVACIDAD DE LA INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

Camerfirma cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos, en particular, ha adaptado sus procedimientos al REGLAMENTO (UE) 2016/679 General de Protección de Datos (RGPD). En este sentido, este documento sirve, de conformidad con la Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. (artículo 8) y el Reglamento eIDAS (artículo 24.2.f) como documento de seguridad.

9.4.2. INFORMACIÓN CONSIDERADA COMO PRIVADA

La información personal sobre un individuo que no está públicamente disponible en los contenidos de un certificado o CRL se considera privada.

9.4.3. INFORMACIÓN NO CONSIDERADA PRIVADA

La información personal sobre un individuo disponible en los contenidos de un certificado o CRL, se considera como no privada al ser necesaria a la prestación del servicio contratado, sin perjuicio de los derechos correspondientes al titular de los datos personales en virtud de la legislación LOPDGDD/RGPD.

9.4.4. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN PRIVADA

Es responsabilidad del responsable del tratamiento proteger adecuadamente la información privada.

9.4.5. AVISO Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Antes de entablar una relación contractual, Camerfirma ofrecerá a los interesados la información previa acerca del tratamiento de sus datos personales y ejercicio de derechos, y en su caso, recabará el consentimiento preceptivo para el tratamiento diferenciado del tratamiento principal para la prestación de los servicios contratados.

9.4.6. DIVULGACIÓN DE CONFORMIDAD CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Los datos personales que sean considerados privados o no, solo podrán divulgarse en caso cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Los descritos en el artículo 6.1 del RGPD o cualquier otra disposición legal que sea aplicable.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

Camerfirma es titular de los derechos de propiedad intelectual sobre esta DPC y CPs, y sobre los certificados electrónicos que emite, salvo acuerdo en otro sentido.

9.6. OBLIGACIONES Y RESPONSABILIDADES CIVILES

9.6.1. OBLIGACIONES Y RESPONSABILIDADES DE LA AC

9.6.1.1. AC

De acuerdo con lo establecido en esta DPC y en las PC, y de acuerdo con la legislación vigente en materia de prestación de servicios de certificación, Camerfirma se compromete a:

- Cumplir con las disposiciones dentro del ámbito de esta DPC y las PCs.
- Proteger sus claves privadas y mantenerlas seguras.
- Emitir certificados de acuerdo con esta DPC y las PC y las normas técnicas aplicables.
- Emitir certificados de acuerdo con la información que posee y que no contengan errores.
- Emitir certificados con el contenido definido por la legislación vigente para los certificados cualificados.
- Publicar los certificados emitidos en un directorio, respetando todas las disposiciones legales en materia de protección de datos.
- Revocar los certificados de acuerdo con esta política y publicar las revocaciones en las CRLs.
- Informar a los sujetos y a otras personas interesadas sobre la revocación de sus certificados, en tiempo y de acuerdo con la legislación vigente.
- Publicar esta DPC y las PC en su sitio web.
- Informar de los cambios en esta DPC y en las PC a los Sujetos, al Suscriptor y a sus ARs asociadas.
- No almacenar ni copiar los datos de creación de firma del Sujeto, salvo en el caso de los certificados de cifrado y cuando esté legalmente previsto o permitido su almacenamiento o copia.
- Proteger los datos utilizados para crear la firma mientras estén custodiados, si es el caso.
- Establecer sistemas de creación y custodia de datos en las actividades mencionadas, protegiendo los datos de su pérdida, destrucción o falsificación.
- Conservar los datos relativos al certificado expedido durante el periodo mínimo exigido por la legislación vigente.

<u>Responsabilidad de Camerfirma:</u>

El Artículo 10 de la Ley 6/2020 de Servicios de Confianza establece que:

"*Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado*"

El Artículo 13 del Reglamento eIDAS establece:

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

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

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

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

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

Camerfirma es responsable de los daños y perjuicios causados a los usuarios de sus servicios, ya sea el Sujeto o la Parte que Confía, y a otros terceros de acuerdo con los términos y condiciones establecidos en la legislación vigente.

En este sentido, Camerfirma es la única responsable en parte de (i) la emisión de los certificados, (ii) la gestión de los mismos a lo largo de su ciclo de vida y (iii) en particular, si es necesario, en caso de revocación de los certificados. En concreto, Camerfirma es fundamentalmente responsable de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión, mediante la confirmación de los datos del solicitante y las prácticas de RA.
- La garantía de que 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 esta DPC.

9.6.2. OBLIGACIONES Y RESPONSABILIDADES DE LA AR

Las AR son entidades que las AC designan para el registro y aprobación de certificados, por lo que las AR también cumplen con las obligaciones definidas en esta DPC y PC para la emisión de certificados y de acuerdo con la legislación vigente, en particular para:

- Cumplir con las disposiciones de esta DPC y de las PC aplicables a cada tipo de certificado emitido.
- Proteger sus claves privadas que utilizan para ejercer sus funciones.
- Respetar los términos del acuerdo firmado con la AC.
- Respetar los Términos y Condiciones firmados por el Sujeto y/o el Suscriptor.

En lo que se refiere al ciclo de vida de los certificados:

- Antes de la emisión del certificado:
    - Comprobar la identidad del Sujeto y/o Suscriptor del certificado según los métodos definidos en esta DPC.
    - Comprobar la exactitud y autenticidad de la información proporcionada por el Solicitante o el Responsable.
    - Informar al Sujeto y/o Suscriptor sobre sus obligaciones, sobre la forma de conservar los datos y del dispositivo de creación de la firma electrónica, y los datos para acceder a los mismos, así como sobre el proceso que debe seguir en caso de mal uso o pérdida del certificado o del dispositivo, los límites de uso, la responsabilidad, etc. y dónde puede acceder para consultar la DPC, las PCs y los Términos y Condiciones.
    - Gestionar y proveer al Sujeto o al Suscriptor o al Responsable el certificado según la DPC y las CP.
    - En su caso, entregar el dispositivo criptográfico correspondiente.
    - Formalizar los Términos y Condiciones y otros documentos contractuales con el Sujeto y/o Suscriptor de manera analógica o utilizando herramientas digitales que permitan la conservación de la aceptación formal.
- Después de la emisión:
    - Conservar los documentos aportados por el Sujeto y/o Suscriptor y los Términos y Condiciones firmados en archivo físico o digital durante el periodo exigido por la legislación vigente.
    - Informar a la AC sobre las causas de revocación, cuando se conozcan.

Por lo tanto, las AR son responsables de las posibles consecuencias debidas al incumplimiento de los deberes de registro, y se comprometen a respetar esta DPC, que las AR deben tener perfectamente controlada y que deben utilizar como guía.

En caso de reclamación por parte de un Sujeto, Suscriptor o Tercero que Confía, las AC deben ofrecer pruebas de que ha actuado con diligencia y si hay pruebas de que la causa de la reclamación se debe a una incorrecta validación o comprobación de los datos, las AC pueden responsabilizar a las AR de las consecuencias, de acuerdo con el convenio firmado con las AR.

Para evitar el incumplimiento de las obligaciones de las AR, las AC controlan periódicamente la actividad de las AR y auditan al menos cada dos (2) años los recursos utilizados y su conocimiento y control sobre los procedimientos operativos utilizados para prestar los servicios de las AR.

Las mismas responsabilidades son asumidas por las AR en virtud de los incumplimientos de las entidades delegadas como los Puntos de Verificación Física (PVF), sin detrimento de su derecho a impugnarlas.

9.6.3. OBLIGACIONES Y RESPONSABILIDADES DEL SUSCRIPTOR

9.6.3.1. SUSCRIPTOR

El suscriptor de un certificado estará obligado a cumplir con lo establecido en la normativa vigente y además a:

- Aceptar los Términos y Condiciones exigidos por el proveedor.
- Informar a la AR o a la AC de cualquier cambio en los datos aportados para la emisión del certificado durante su periodo de validez.
- Informar a la AR o a la AC lo antes posible de la existencia de cualquier causa de revocación.

9.6.3.2. SOLICITANTE

El Solicitante de un certificado está obligado a cumplir con lo establecido en la normativa vigente y además:

- Proporcionar a la AR la información necesaria para llevar a cabo una correcta identificación.
- Garantizar la exactitud y veracidad de la información proporcionada.
- Notificar a la AR o a la AC de cualquier cambio en los datos aportados para la emisión del certificado durante su periodo de validez.
- Informar a la AR o a la AC lo antes posible de la existencia de cualquier causa de revocación.
- Proporcionar la información del Sujeto (Firmante)/Solicitante/Responsable bajo las normas impuestas por la ley de protección de datos.

9.6.3.3. SUJETO/TITULAR/RESPONSABLE

El Sujeto/Titular y el Responsable si es distinto al Sujeto/Titular, estarán obligados a cumplir con lo establecido en la normativa vigente y además:

- Aceptar los Términos y Condiciones exigidos por el proveedor.
- Utilizar el certificado tal y como se establece en las DPC y CPs vigentes.
- Respetar las condiciones de los documentos firmados con Camerfirma, las AC y las AR.
- Hacer uso del certificado digital de forma personal e intransferible y custodiar los datos de activación de la clave privada de forma diligente. El Sujeto/Titular y el Responsable serán los únicos responsables ante la Entidad que representan y la Parte que Confía en caso de no contar con la debida autorización, así como de las consecuencias que se deriven de un uso indebido o no debidamente supervisado.
- Informar a la AR o a la AC lo antes posible de la existencia de cualquier causa de revocación.
- Notificar a la AR o a la AC de cualquier cambio en los datos aportados para la emisión del certificado durante su periodo de validez.
- No utilizar la clave privada ni el certificado desde el momento en que se solicite o se le avise por la AC o la AR de la revocación del mismo, o una vez haya expirado el plazo de validez del certificado.
- Autorizar a la AC y a la AR para que procedan al tratamiento de los datos personales contenidos en los certificados, en el marco de las finalidades de la relación telemática y, en todo caso, para el cumplimiento de las obligaciones legales de verificación de los certificados.
- Ser responsable de que toda la información que se incluya, por cualquier medio, en la solicitud del certificado y en el propio certificado sea exacta, completa a efectos del mismo y esté actualizada en todo momento.
- Informar inmediatamente a la AC o a la AR de cualquier inexactitud en el certificado detectada una vez emitido, así como de cualquier cambio en la información proporcionada en la emisión del certificado.
- En el caso de los certificados en un dispositivo hardware, en el caso de que éste pierda su posesión, ponerlo en conocimiento de la AR o de la AC a la mayor brevedad posible y, en todo caso, dentro de las 24 horas siguientes a la producción de la citada circunstancia, con independencia del hecho concreto que lo haya originado o de las actuaciones que eventualmente pueda ejercer.

- No utilizar la clave privada, el certificado electrónico o cualquier otro soporte técnico proporcionado por la AC o la AR para realizar cualquier transacción prohibida por la legislación aplicable.

Además, el Sujeto/Titular y el Responsable deberán ser especialmente diligentes en la custodia de la clave privada y del dispositivo cualificado de creación de firma, para evitar su uso no autorizado.

9.6.4. OBLIGACIONES Y RESPONSABILIDADES DE LA PARTE QUE CONFÍA

Será obligación de la Parte Contratante cumplir con lo establecido en la normativa vigente y, además:

- Verifique el estado de los certificados, ya sea consultando las CRL o los servicios OCSP, y la no caducidad de los mismos antes de realizar cualquier operación basada en ellos.
- Conocer y someterse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar someterse a las mismas. En el caso de certificados para un Representante Apoderado de una Persona Jurídica o una Persona No Jurídica que implica una relación de representación basada en un poder especial o documento privado con facultades limitadas, las partes que confían deben comprobar los límites de dichas facultades.
- Verificar que el certificado está cualificado comprobando que el certificado ha sido firmado con la clave privada asociada a un certificado de AC válido de Camerfirma incluido en la Lista de Confianza Española que esté en vigor, de acuerdo con lo establecido en el artículo 22 del Reglamento eIDAS y en la Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relativos a las listas de confianza de conformidad con el artículo 22.5 del Reglamento eIDAS.

9.6.5. OBLIGACIONES Y RESPONSABILIDADES DE OTROS PARTICIPANTES

En el caso de aquellos certificados que impliquen una vinculación entre una persona física y una Entidad, la Entidad estará obligada a solicitar a la AC o a la AR la revocación del certificado cuando la persona física deje de estar vinculada a la Entidad.

9.7. EXENCIÓN DE GARANTÍAS

De acuerdo con la legislación vigente, la responsabilidad asumida por las ACs y las ARs no se aplica en los casos en los que el uso indebido de los certificados sea causado por acciones imputables al Solicitante, al Sujeto, al Responsable y a la Parte que Confía debido a:

- No haber proporcionado la información correcta, inicial o posteriormente como consecuencia de cambios en las circunstancias descritas en el certificado digital, cuando la AC o la AR no hayan podido detectar la inexactitud de los datos.
- Haber actuado de forma negligente en cuanto al almacenamiento de los datos utilizados para crear la firma y mantenerlos confidenciales.
- No haber solicitado la revocación de los datos del certificado digital en caso de que surjan dudas sobre su conservación o confidencialidad.
- Haber empleado la firma una vez que el certificado digital ha caducado;
- Exceder los límites establecidos en el certificado digital.
- Acciones imputables a la Parte que Confía, si ésta actúa de forma negligente, es decir, cuando no comprueba o tiene en cuenta las restricciones establecidas en el certificado en relación con el uso permitido y el número limitado de transacciones, o cuando no tiene en cuenta la situación de validez del certificado.
- Los daños y perjuicios causados al Sujeto, a la Entidad o a las Partes que Confían en él por la inexactitud de los datos incluidos en el certificado digital, si estos datos se han acreditado mediante un documento público inscrito en un registro público, si es necesario.
- Un uso inadecuado o fraudulento del certificado en caso de que el Sujeto/Titular y/o el Responsable lo haya cedido o autorizado su uso a favor de un tercero siendo responsabilidad exclusiva del Sujeto/Titular y del Responsable el control de las claves asociadas al certificado.

Camerfirma y las ARs no se responsabilizan de forma alguna en el caso de que se produzca alguna de las siguientes circunstancias:

- Guerra, catástrofes naturales o cualquier otro caso de fuerza mayor.
- El uso de certificados vulnerando la legislación vigente, la DPC y/o las PCs.

- Uso indebido o fraudulento de certificados, CRLs o respuestas OCSP.
- Uso de la información contenida en los certificados, CRLs o respuestas OCSP.
- Daños causados durante la comprobación de los motivos de revocación.
- Debido al contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Fallo en la recuperación de documentos encriptados con la clave pública del Sujeto.

9.8. LIMITACIÓN DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

9.8.1. LIMITACIONES DE RESPONSABILIDAD DE LA AC

Camerfirma es responsable del incumplimiento de las disposiciones de la DPC y, en su caso, de las disposiciones del Reglamento eIDAS y de la Ley 6/2020.

Camerfirma no garantiza los algoritmos y estándares criptográficos utilizados y no será responsable de los daños causados por ataques externos a los mismos, siempre que se haya aplicado la debida diligencia según el estado del arte en cada momento, y se haya actuado de acuerdo con lo establecido en esta DPC y en el Reglamento eIDAS y la Ley 6/2020.

Camerfirma será responsable de los daños causados al Suscriptor o al Sujeto o a cualquier Tercero que Confíe, siempre que exista fraude o negligencia grave, en relación con:

- La garantía de que la clave pública y la privada funcionan de forma combinada y complementaria.
- La exactitud de la información incluida en el certificado en la fecha de emisión, siempre que coincida con la información verificada.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad establecida por la legislación vigente aplicable.

9.8.2. LIMITACIONES DE RESPONSABILIDAD DE LA AR

La AR será plenamente responsable del procedimiento de identificación y autentificación de los Suscriptores, Solicitantes, Sujetos o Responsables. Lo hará de acuerdo con lo establecido en la presente DPC.

Si la generación del par de claves no se realiza en presencia del Sujeto/Titular o del Responsable, la AR será responsable de la custodia de las claves hasta su entrega al Sujeto/Titular o al Responsable.

9.8.3. LIMITACIONES DE RESPONSABILIDAD DEL SUSCRIPTOR/SOLICITANTE/SUJETO/TITULAR/RESPONSABLE

Es de exclusiva responsabilidad del Suscriptor/Solicitante/Sujeto/Titular/Responsable el cumplimiento de las obligaciones estipuladas en este documento y en los documentos legales firmados por ellos.

9.8.4. LIMITACIONES DE RESPONSABILIDAD DE CAMERFIRMA

Camerfirma no será responsable en ningún caso por las siguientes circunstancias:

- Estado de guerra, catástrofes naturales, mal funcionamiento de los servicios eléctricos, de las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor/Solicitante/Sujeto/Titular/Responsable, o por las Partes que Confían o cualquier otro caso de fuerza mayor.
- En su caso, por el uso indebido de los repositorios de certificados emitidos por las ACs.
- Uso indebido de la información contenida en los certificados, en las CRLs o en los servicios OCSP.
- En lo referente al contenido de los mensajes o documentos firmados o cifrados por los certificados.
- En lo referente a las acciones o inacciones del Suscriptor/Solicitante/Sujeto/Titular/Responsable:
    - Falta de exactitud o veracidad de la información proporcionada para emitir el certificado.
    - Retraso en la notificación de los motivos de revocación del certificado.
    - No solicitar la revocación del certificado cuando corresponda.
    - Negligencia en la conservación de sus datos de creación de la firma electrónica, la información para acceder a los datos de creación de la firma electrónica, el aseguramiento de su confidencialidad y la protección contra cualquier acceso o divulgación.
    - Utilización del certificado más allá de su período de validez o cuando la AC notifica la revocación del certificado.

- Exceder los límites de uso del certificado, estipulados en la normativa vigente y en esta DPC y PC o no utilizarlo de acuerdo con las condiciones establecidas y comunicadas al Suscriptor/Solicitante/Sujeto/Titular/Responsable.

- En relación con las acciones o inacciones de la Parte que Confía en el certificado:
  - No verificar las restricciones contenidas en el certificado o en esta DPC y en las PCs respecto a sus posibles usos.
  - No comprobar la fecha de caducidad del certificado indicada en la extensión de la validez del certificado o no verificar la firma digital.

9.9. INDEMNIZACIONES

El seguro cubrirá todas las cantidades que Camerfirma deba pagar legalmente, hasta el límite de cobertura contratado, como consecuencia de cualquier procedimiento judicial en el que se declare su responsabilidad.

9.10. PLAZO Y CESE

9.10.1. PLAZO

Ver sección 5.8.

9.10.2. CESE

Ver sección 5.8.

9.10.3. EFECTO DEL CESE

Ver sección 5.8.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

Cualquier notificación en relación con esta DPC se hará por correo electrónico o por correo certificado a cualquiera de las direcciones indicadas en la sección 1.5.2.

9.12. MODIFICACIONES

9.12.1. PROCEDIMIENTO PARA MODIFICACIONES

Camerfirma se reserva el derecho a modificar este documento por razones técnicas o para reflejar cualquier cambio en los procedimientos que se haya producido por exigencias legales, normativas (Reglamento eIDAS, Foro CA/B, Organismos de Supervisión, etc.) o como consecuencia de la optimización del ciclo de trabajo. Cada nueva versión de este documento sustituye a todas las versiones anteriores, que siguen siendo, sin embargo, aplicables a los certificados emitidos mientras esas versiones estaban en vigor. Se publicará al menos una actualización anual. Estas actualizaciones se reflejarán en el historial de versiones del documento, al final del mismo.

Los cambios que se puedan realizar en este documento no requieren notificación, salvo que afecten directamente a los derechos del Suscriptor/Sujeto/Titular/Responsable/Partes que Confían, en cuyo caso podrán ser notificados en un plazo de 15 días a través de la página web de Camerfirma.

9.12.2. MECANISMO DE NOTIFICACIÓN Y PLAZOS

9.12.2.1. LISTA DE ELEMENTOS

Cualquier elemento de este documento puede ser modificado sin previo aviso.

9.12.2.2. MÉTODO DE NOTIFICACIÓN

Cualquier cambio propuesto en este documento se publica inmediatamente en el sitio web de Camerfirma https://policy21.camerfirma.com

Este documento contiene una sección de cambios y versiones, en la que se especifican los cambios que se han producido desde su creación y las fechas de los mismos.

Los cambios en este documento se comunican expresamente a las entidades que confían y entidades que emiten certificados en virtud de esta DPC y PC. Especialmente los cambios en esta DPC y PC serán notificados al Organismo de Supervisión.

9.12.2.3. PERIODO DE COMENTARIOS

Los Suscriptores/Sujetos/Responsables y Partes que Confían pueden presentar sus comentarios a la organización de gestión de la política dentro de los 15 días siguientes a la recepción de la notificación.

9.12.2.4. MECANISMO DE TRATAMIENTO DE LOS COMENTARIOS

Cualquier medida que se tome como resultado de los comentarios queda a discreción del AP.

9.12.3. CIRCUNSTANCIAS EN LAS QUE SE DEBE CAMBIAR EL OID

No estipulado.

9.13. PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

En caso de cualquier controversia o conflicto derivado de las presentes DPC y Términos y Condiciones, las partes, con renuncia a cualquier otra jurisdicción que pudiera corresponderles, se someten a los Juzgados y Tribunales de Madrid, salvo que el reclamante sea un consumidor, por lo que será competente el Juez o Tribunal que corresponda al domicilio del consumidor.

9.14. LEGISLACIÓN APLICABLE

La ejecución, interpretación, modificación o vigencia de esta DPC y PCs está obligada a cumplir los requisitos establecidos en la legislación española y de la Unión Europea vigente en cada momento.

9.15. CONFORMIDAD CON LA LEGISLACIÓN APLICABLE

Ver sección 9.14.

9.16. CLAUSULAS DIVERSAS

9.16.1. ACUERDO COMPLETO

El Firmante y las Partes que Confían en los Certificados asumen en su totalidad el contenido de esta DPC y CPs.

9.16.2. ASIGNACIÓN

Las entidades que participan en esta DPC no podrán ceder ninguno de sus derechos u obligaciones en virtud de esta DPC o de los acuerdos aplicables sin el consentimiento por escrito de Camerfirma.

9.16.3. SEPARABILIDAD

Si las disposiciones individuales de esta DPC resultan ineficaces o incompletas, esto se hará sin perjuicio de la efectividad de todas las demás disposiciones.

La disposición ineficaz será reemplazada por una disposición efectiva que se considera que refleja más de cerca el sentido y el propósito de la disposición ineficaz. En el caso de disposiciones incompletas, se acordará una modificación que se considere que corresponde a lo que razonablemente se habría acordado de acuerdo con el sentido y los propósitos de esta DPC, si el asunto se hubiera considerado de antemano.

9.16.4. CUMPLIMIENTO (HONORARIOS DE ABOGADOS Y EXENCIÓN DE DERECHOS)

Camerfirma puede solicitar una indemnización y honorarios de abogados de una parte por daños, pérdidas y gastos relacionados con la conducta de dicha parte. El hecho de que Camerfirma no haga cumplir una disposición de esta CPS no elimina el derecho de Camerfirma de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de esta DPC. Para ser efectiva, cualquier renuncia debe estar por escrito y firmada por Camerfirma.

ANEXO I: HISTORIA DEL DOCUMENTO

19/01/2022	V1.0.0	Versión inicial