Tinexta Infocert

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CAMERFIRMA

Versión 2.0

Redacción y Revisión: Departamentos de Cumplimiento y Jurídico de Camerfirma

Aprobación (AP): Departamento Jurídico de Camerfirma

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

Este documento se puede obtener en la dirección:
https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

Idioma: Castellano

Código: PUB-2022-18-03

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2025.05.29 15:43:04 +02'00'

INDICE

1 INTRODUCCIÓN

1.1 VISIÓN GENERAL

Camerfirma es un Prestador de Servicios Electrónicos de Confianza (PSC) cualificado en la Unión Europea, especializado en la emisión de certificados digitales y soluciones de firma electrónica. Fue creado por las Cámaras de Comercio de España y ofrece servicios de identidad digital para empresas, autónomos y Administraciones Públicas.

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).

El presente documento constituye la Declaración de Prácticas de Certificación (en adelante, DPC) que es el conjunto de prácticas adoptadas para la solicitud, emisión, gestión, revocación y renovación de certificados electrónicos. Contiene información detallada sobre sus sistemas de seguridad, soporte, administración, emisión (incluida la renovación con o sin cambio de claves) y revocación de certificados, así como sobre la relación de confianza entre la AC, el Titular, y la Parte que Confía. Describe de forma precisa los servicios prestados, procedimientos detallados de la gestión del ciclo de vida de los certificados, etc.

La estructura de este documento sigue las directrices del estándar RFC3647 - *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*, desarrollado por el grupo de trabajo PKIX del IETF.

Para cada tipo de certificado emitido por Camerfirma se han elaborado las Políticas de Certificación que recogen condiciones y requerimientos específicos de cada uno de ellos (en adelante PC), que se encuentran publicadas en la web.

Aunque los documentos DPC y CP's son esenciales para describir y gestionar las políticas y prácticas de certificados, muchos usuarios de PKI, especialmente los consumidores, encuentran estos documentos difíciles de entender. En consecuencia, existe la necesidad de un instrumento complementario y simplificado que pueda ayudar a los usuarios de PKI a tomar decisiones de confianza informadas. Para ello, Camerfirma publica para cada tipo de certificado un documento denominado "Texto de Divulgación o PDS" que recoge de forma simplificada la información más relevante de los certificados emitidos. No obstante, dichas declaraciones de divulgación no pretenden sustituir a la DPC ni a las CP's.

El presente documento especifica la DPC y las PC para la emisión de certificados por las AC activas de AC Camerfirma SA (en adelante, Camerfirma) bajo las jerarquías de Camerfirma de 2008, 2016, 2021, 2024 (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016, CAMERFIRMA ROOT 2021) y 2024 (INFOCERT-CAMERFIRMA ROOT 2024), de acuerdo con el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo de 11 de abril de 2024 por el que se modifica el Reglamento (UE) n.o 910/2014 en lo que respecta

al establecimiento del marco europeo de identidad digital (en adelante el Reglamento eIDAS) y en base a los siguientes estándares ETSI:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements.
- ETSI TS 119 431-1: Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev
- ETSI TS 119 431-2: Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

Adicionalmente, la DPC y las PC en este documento cumplen con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, Ley 6/2020).

Para certificados de entidad final emitidos a personal al servicio de las Administraciones Públicas españolas, Camerfirma tiene en cuenta también lo estipulado en el documento titulado “Perfiles de certificados electrónicos 2.0” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas en el marco de las leyes españolas 39/2015 y 40/2015.

Con respecto a las PC que deben aplicarse de acuerdo con ETSI EN 319 411-1 y ETSI EN 319 411-2, se incluyen en las PC en este documento:

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

  NCP — Política de Certificación Normalizada. Cumple las mejores prácticas generales reconocidas para prestadores de servicios de confianza que emiten certificados utilizados para respaldar cualquier tipo de transacción.

  NCP+ — Política de Certificación Normalizada Extendida. NCP que requiere un dispositivo criptográfico seguro. Incluye todos los requisitos de la política NCP, más requisitos adicionales adecuados para soportar el uso de un dispositivo criptográfico seguro (para firmar y/o descifrar).

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

  QCP-n — Política de Certificación para Certificados Cualificados en la UE emitidos a personas físicas. Incluye todos los requisitos de la política NCP, más

requisitos adicionales adecuados para soportar la emisión y la gestión de certificados cualificados en la UE, tal como se especifican en el Reglamento eIDAS. Si la implementación requiere un dispositivo criptográfico seguro, incluye todos los requisitos de la política NCP+, más requisitos adicionales adecuados para soportar la emisión y la gestión de certificados cualificados en la UE, tal como se especifican en el Reglamento eIDAS. Los certificados emitidos bajo estos requisitos tienen como objetivo respaldar las firmas electrónicas avanzadas basadas en un certificado cualificado definidas en los artículos 26 y 28 del Reglamento eIDAS.

QCP-n-qscd Política de Certificación para 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+), más requisitos adicionales adecuados para soportar la emisión y la gestión de certificados cualificados en la UE, tal como se especifican en el Reglamento eIDAS, incluidos los específicos del suministro de QSCD. Los certificados emitidos bajo estos requisitos tienen como objetivo respaldar las firmas electrónicas cualificadas, tal como se definen en el artículo 3 (12) del Reglamento eIDAS.

QCP-l Política de Certificación para Certificados Cualificados en la UE emitidos a personas jurídicas. Incluye todos los requisitos de la política NCP, más requisitos adicionales adecuados para soportar la emisión y la gestión de certificados cualificados en la UE, tal como se especifican en el Reglamento eIDAS. Si la implementación requiere un dispositivo criptográfico seguro, incluye todos los requisitos de la política NCP+, más requisitos adicionales adecuados para soportar la emisión y gestión de certificados cualificados en la UE, tal como se especifica en el Reglamento eIDAS. Los certificados emitidos bajo estos requisitos tienen como objetivo respaldar los sellos electrónicos avanzados basados en un certificado cualificado definidos en los artículos 36 y 38 del Reglamento eIDAS.

QCP-l-qscd Política de Certificación para Certificados Cualificados en la UE emitidos a personas jurídicas 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-l (incluidos todos los requisitos de la política NCP+), más requisitos adicionales adecuados para soportar la emisión y la gestión de certificados cualificados en la UE, tal como se especifican en el Reglamento eIDAS, incluidos los específicos del suministro de QSCD. Los certificados emitidos bajo estos requisitos tienen como objetivo respaldar los sellos electrónicos cualificados, tal como se definen en el artículo 3 (27) del Reglamento eIDAS.

Las AC bajo la DPC en este documento (en adelante, esta DPC) emiten certificados cualificados en dispositivos QSCD y en dispositivos No QSCD y certificados no cualificados en dispositivos No QSCD –en el caso de certificados de entidad final, bajo las PC en este documento (en adelante, estas

PC)–, con claves generadas en:

- QSCD Tarjeta/Token:
  - Tarjetas criptográficas QCSD.
  - Tokens criptográficos QCSD.
- QSCD Nube:
  - Plataforma centralizada QCSD gestionada por Camerfirma u otro PCSC.
- QSCD HSM:
  - HSM QSCD gestionado por Camerfirma u otro PSC. Solo para certificados de TSU.
- No QSCD:
  - P12:
    - Software (PKCS #12).
  - CSR:
    - Dispositivo externo No QSCD o QSCD no gestionado por Camerfirma. A través de una petición de firma de certificado en formato PKCS #10.
  - Tarjeta/Token (dispositivo criptográfico seguro):
    - Tarjetas criptográficas No QSCD o QSCD.
    - Tokens criptográficos No QSCD o QSCD.
  - Nube (dispositivo criptográfico seguro):
    - Plataforma centralizada No QSCD o QSCD gestionada por Camerfirma u otro PSC.
  - HSM (dispositivo criptográfico seguro):
    - HSM No QSCD o QSCD gestionado por Camerfirma u otro PSC. Solo para certificados de TSU, AC y OCSP.

Adicionalmente, para garantizar la ciberseguridad y la ciberresiliencia de los servicios amparados en esta DPC, Camerfirma ha alineado sus operaciones a los requisitos de seguridad de redes y de la información establecidos en la Directiva (UE) 2555/2022 (Directiva NIS2) y su Reglamento de Ejecución (UE) 2024/2690; así como, a la normativa de desarrollo que se dicte incluida la normativa de transposición al ordenamiento jurídico español.

1.2 IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

Nombre:	Declaración de Prácticas de Certificación de CAMERFIRMA
Descripción:	Declaración de Prácticas de Certificación para las AC activas de Camerfirma bajo las jerarquías de Camerfirma de 2008, 2016, 2021 y 2024 (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016,

	CAMERFIRMA ROOT 2021) y 2024 (INFOCERT-CAMERFIRMA ROOT 2024)
Versión:	Ver página inicial
OID:	Jerarquías Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016 ○ 1.3.6.1.4.1.17326.10.9.8: HSM Jerarquía CAMERFIRMA ROOT 2021 ○ 1.3.6.1.4.1.17326.10.21.0.1: HSM
Localización:	https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

1.3 PARTICIPANTES EN LA PKI

1.3.1 PRESTADOR DE SERVICIOS ELECTRÓNICOS DE CONFIANZA (PSC)

Camerfirma es un Prestador de Servicios Electrónicos de Confianza (PSC) que emite y gestiona certificados digitales. Su función principal es garantizar la identidad de personas, empresas o sistemas en entornos digitales, permitiendo la autenticación, la firma electrónica y el cifrado seguro de información.

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

Nombre corporativo:	AC CAMERFIRMA, S.A.
NIF:	A82743287
Domicilio social:	Calle de Rodríguez Marín 88 – 28016 Madrid
Teléfono:	+34 91 136 91 05
Email:	ca@camerfirma.com / info@camerfirma.com
Página web:	https://www.camerfirma.com

Camerfirma utiliza Autoridades de Registro (en adelante, AR) con el fin de comprobar la identidad de los solicitantes/suscriptores de certificados y almacenar la documentación relativa al contenido de los certificados de entidad final, por cuenta de la Autoridad de Certificación.

1.3.2 AUTORIDAD DE CERTIFICACIÓN (AC)

Un PSC puede incorporar una o más jerarquías de AC. Una jerarquía de AC incluye una AC Raíz y una o más AC Subordinadas (también conocidas como AC Intermedias).

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

El uso de jerarquías de AC reduce los riesgos que conlleva la emisión de certificados y su organización en las diferentes AC. Las claves de las AC Subordinadas 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 Subordinada obtiene un certificado de la AC Raíz para emitir certificados de entidad final y/u otros certificados de AC Subordinada. El número de AC Subordinadas permitidas bajo una AC Raíz o Subordinada se especifica en la extensión *Basic Constraints* (campo *pathLenConstraint*) del certificado de la AC.

A continuación, se describen las jerarquías de AC que Camerfirma gestiona como propietaria bajo esta DPC. En el caso de AC Subordinadas propiedad de otra organización (en adelante, AC Subordinada/s externas/s), esta DPC hace referencia a su existencia dentro de la jerarquía correspondiente debido a su subordinación a la AC Raíz o a una AC Subordinada propiedad de Camerfirma, pero se regirá por sus propias DPC y PC.

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 las siguientes jerarquías de AC:

- CHAMBERS OF COMMERCE ROOT
- GLOBAL CHAMBERSIGN ROOT
- CAMERFIRMA ROOT 2021
- INFOCERT-CAMERFIRMA ROOT 2024

1.3.2.1 JERARQUÍAS CHAMBERS OF COMMERCE ROOT

CHAMBERS OF COMMERCE ROOT en sus distintas versiones es propiedad de AC CAMERFIRMA SA, tal como se indica en el atributo *Organización* del campo *Sujeto* de los certificados de AC Raíz correspondientes.

Estas jerarquías están diseñadas para desarrollar una red de confianza con el objetivo de emitir certificados a personas físicas, con o sin atributos de vinculación a entidades públicas o privadas, y a entidades públicas o privadas dentro del territorio de la Unión Europea, y donde las AC están establecidas en España, y las AR son gestionadas por las Cámaras de Comercio, Industria y Navegación de España o por entidades públicas o privadas sin limitación territorial.

Bajo estas jerarquías se permite la emisión de certificados por AC Subordinadas establecidas en España correspondientes a un colectivo empresarial, colegial o público concreto, siempre que las AC y las AR cumplan los requisitos establecidos por Camerfirma, sujetándose en todo caso a la legislación y a la normativa vigentes aplicables.

Las AC Subordinadas que emiten certificados bajo estas jerarquías pueden ser propiedad de Camerfirma o de otros PSC. Todas las AC que operan bajo estas jerarquías lo hacen desde

infraestructuras controladas técnicamente por Camerfirma.

Los datos de identificación de los certificados de AC Raíz activas de estas jerarquías son:

- **CHAMBERS OF COMMERCE ROOT – 2016**

  CN: CHAMBERS OF COMMERCE ROOT - 2016

  Válido desde (hora UTC): 14/04/2016 07:35:48

  Válido hasta (hora UTC): 08/04/2040 07:35:48

  Número de Serie: 349A 2DA1 8206 B2B3

  ***X509v3 Subject Key Identifier*:** 9E2E 654F 3E57 F5AB 7D96 C68B DFB3 356D 4AE8 9E8B

  ***Hash SHA-1*:** 2DE1 6A56 77BA CA39 E1D6 8C30 DCB1 4ABE 22A6 179B

  ***Hash SHA-256*:** 04F1 BEC3 6951 BC14 54A9 04CE 3289 0C5D A3CD E135 6B79 00F6 E62D FA20 41EB AD51

- **Chambers of Commerce Root – 2008** (certificado con firma SHA-1)

  CN: Chambers of Commerce Root - 2008

  Válido desde (hora UTC): 01/08/2008 12:29:50

  Válido hasta (hora UTC): 31/07/2038 12:29:50

  Número de Serie: 00 A3DA 427E A4B1 AEDA

  ***X509v3 Subject Key Identifier*:** F924 AC0F B2B5 F879 C0FA 6088 1BC4 D94D 029E 1719

  ***Hash SHA-1*:** 786A 74AC 76AB 147F 9C6A 3050 BA9E A87E FE9A CE3C

  ***Hash SHA-256*:** 063E 4AFA C491 DFD3 32F3 089B 8542 E946 17D8 93D7 FE94 4E10 A793 7EE2 9D96 93C0

- **Chambers of Commerce Root – 2008** (certificado con las mismas claves y firma SHA-256)

  CN: Chambers of Commerce Root - 2008

  Válido desde (hora UTC): 07/12/2011 11:28:07

  Válido hasta (hora UTC): 31/07/2038 11:28:07

  Número de Serie: 00 D908 3FBB A967 CA1A

  ***X509v3 Subject Key Identifier*:** F924 AC0F B2B5 F879 C0FA 6088 1BC4 D94D 029E 1719

  ***Hash SHA-1*:** CD03 B468 3048 E364 B8E9 F7ED D94C 7874 7C39 51CA

  ***Hash SHA-256*:** 3666 F804 9140 FDC0 A65E 809B 281A 3BE3 B10D AFEE FD76 B9DD C272 A93E 83CA 5B99

En la PC de cada tipo de certificado se indica el esquema de AC Raíces y AC Subordinadas activas bajo estas jerarquías, incluyendo, en su caso, los respectivos OID en la extensión *Certificate Policies* de los certificados de cada AC y/o de los distintos tipos de certificados de entidad final activos emitidos por cada AC Subordinada bajo cada PC.

A continuación, se describen las AC Subordinadas bajo esta DPC dentro de las jerarquías CHAMBERS OF COMMERCE ROOT, y, en su caso, las correspondientes PC de los certificados emitidos activos, excepto la PC de los certificados OCSP (ver sección 1.3.1.5).

1.3.2.1.1 AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Esta AC Subordinada emite certificados cualificados y no cualificados a personas físicas dentro de la UE, de acuerdo con los requisitos del Reglamento eIDAS y la Ley 6/2020.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía CHAMBERS OF COMMERCE ROOT – 2016) son:

CN: AC CAMERFIRMA FOR NATURAL PERSONS - 2016

Válido desde (hora UTC): 14/04/2016 08:48:09

Válido hasta (hora UTC): 09/03/2040 08:48:09

Número de Serie: 5151 4CB4 4FA4 54F5

***X509v3 Subject Key Identifier*:** 70B8 F824 C751 CACE 2280 9208 C9C0 682F C147 5851

***Hash SHA-1*:** 171A 2ADB 87CA 5927 047A 6E76 9757 3877 B5D6 02E5

***Hash SHA-256*:** EEDD 457A F135 3D76 F48E 7C61 23F3 9140 E5F9 A069 CA51 B43E EA86 15C9 CEC0 D4BB

1.3.2.1.2 AC CAMERFIRMA FOR LEGAL PERSONS - 2016

Esta AC Subordinada emite certificados cualificados a personas jurídicas dentro de la UE, de acuerdo con los requisitos del Reglamento eIDAS y la Ley 6/2020.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía CHAMBERS OF COMMERCE ROOT – 2016) son:

CN: AC CAMERFIRMA FOR LEGAL PERSONS – 2016

Válido desde (hora UTC): 14/04/2016 08:33:07

Válido hasta (hora UTC): 09/03/2040 08:33:07

Número de Serie: 54B1 6EE1 1124 5A42

***X509v3 Subject Key Identifier*:** C327 8593 D72F 96C5 1BAC 7633 D986 A24A 7D68 1442

***Hash SHA-1*:** EBEE 22EB A7AC 3F68 0175 1756 2414 61D7 D749 E730

***Hash SHA-256*:** 3A80 6626 6D28 BD28 CCD0 F564 C8FB C121 9B4F FAE4 03E0 1E50 39D3 0F24 00F0 EB09

1.3.2.1.3 AC CAMERFIRMA TSA - 2016, CAMERFIRMA TSA II - 2014

Estas AC Subordinadas emiten certificados a personas jurídicas para la firma digital de sellos de tiempo.

Los datos de identificación de los certificados de estas AC Subordinadas (emitido por la AC Raíz de la jerarquía Chambers of Commerce Root – 2008) son:

- **AC CAMERFIRMA TSA – 2016** (emitido por la AC Raíz de la jerarquía CHAMBERS OF COMMERCE ROOT – 2016)

  CN: AC CAMERFIRMA TSA - 2016

  Válido desde (hora UTC): 14/04/2016 10:42:09

  Válido hasta (hora UTC): 09/03/2040 10:42:09

  Número de Serie: 15B7 A58A 54FF 0282

  ***X509v3 Subject Key Identifier*:** 1E6D B5C6 3FEF 9255 5E37 FADB FD10 AABA D93B 4E2C

  ***Hash SHA-1*:** 907F 23C8 E03C 7837 436E 1FB0 3743 7751 75B7 02E6

  ***Hash SHA-256*:** BAAE 2C63 3885 7D50 200F 6F73 DD45 E65A A2D8 95BE D467 5B6E 396B 7222 E018 A9B8

La AC Subordinada AC CA CAMERFIRMA TSA – 2016 no emite nuevos certificados, a excepción del certificado de OCSP.

- **Camerfirma TSA II – 2014** (emitido por la AC Raíz de la jerarquía Chambers of Commerce Root – 2008)

  CN: Camerfirma TSA II - 2014

  Válido desde (hora UTC): 16/12/2014 16:45:33

  Válido hasta (hora UTC): 15/12/2037 16:45:33

  Número de Serie: 25A4 54BC 3455 1238

  ***X509v3 Subject Key Identifier*:** 17C5 40BC 2AF8 45B8 AB33 BFF8 6F49 6CF6 17CA B7D4

  ***Hash SHA-1*:** 19EB DCED EDEB C925 1F3A 098F F4C9 51AE 5552 48B1

  ***Hash SHA-256*:** 6569 5D50 0117 FD72 70F1 027E D121 F059 4267 0075 461D 337E EEC7 F6A5 B757 A47A

1.3.2.1.4 CAMERFIRMA CODESIGN II - 2014

Esta AC Subordinada emite certificados a personas jurídicas para la firma de código.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía Chambers of Commerce Root – 2008) son:

CN: Camerfirma Codesign II - 2014

Válido desde (hora UTC): 16/12/2014 12:25:43

Válido hasta (hora UTC): 15/12/2037 12:25:43

Número de Serie: 6451 2A01 FB00 554A

***X509v3 Subject Key Identifier*:** C4A3 D3EA 633D 4961 DA91 C919 D91B 3335 7875 389F

***Hash SHA-1*:** 247D 88C9 5017 7261 1BB1 5A35 61A7 72DA A16F 2950

***Hash SHA-256*:** 3B0B 2D29 9AF7 74D6 C332 B2BF ABB4 5F44 D866 432B 9552 EA09 4D52 9B6E D125 048B

1.3.2.1.5 CAMERFIRMA CORPORATE SERVER II – 2015

Esta AC Subordinada emite certificados a personas jurídicas.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía Chambers of Commerce Root – 2008) son:

CN: Camerfirma Corporate Server II - 2015

Válido desde (hora UTC): 15/01/2015 09:21:16

Válido hasta (hora UTC): 15/12/2037 09:21:16

Número de Serie: 621F F31C 489B A136

***X509v3 Subject Key Identifier*:** 63E9 F0F0 5600 6865 B021 6C0E 5CD7 1908 9D08 3465

***Hash SHA-1*:** FE72 7A78 EA0C 0335 CDDA 9C2E D75F D4D4 6F35 C2EF

***Hash SHA-256*:** 66EA E270 9B54 CDD1 6931 77B1 332F F036 CDD0 F723 DB30 39ED 3115 55A6 CBF5 FF3E

1.3.2.1.6 CAMERFIRMA AAPP II – 2014

Esta AC Subordinada emite certificados a personas físicas y personas jurídicas de las Administraciones Públicas.

Esta AC Subordinada no emite nuevos certificados.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía Chambers of Commerce Root – 2008) son:

CN: Camerfirma AAPP II - 2014

Válido desde (hora UTC): 16/12/2014 11:59:01

Válido hasta (hora UTC): 15/12/2037 11:59:01

Número de Serie: 1548 D054 B8A8 42BA

***X509v3 Subject Key Identifier*:** 5DA1 55A4 DC4A AC83 11F9 AA38 E5F7 684A FE15 154C

***Hash SHA-1*:** E95E CC41 4D56 452A E354 09AC D23F 34A2 7BDB D26E

***Hash SHA-256*:** 7239 D2F7 70FA FF3B 1CF8 BE2A 05EC 03ED EAAC 053B 554F 90D3 6921 155B A805 1981

La AC Subordinada Camerfirma AAPP II - 2014 no emite nuevos certificados, a excepción del certificado de OCSP.

1.3.2.2 *JERARQUÍAS GLOBAL CHAMBERSIGN ROOT*

GLOBAL CHAMBERSIGN ROOT en sus distintas versiones es propiedad de AC Camerfirma sa tal como se indica en el atributo *Organización* del campo *Sujeto* de los certificados de AC Raíz correspondientes.

Estas jerarquías están diseñadas para la emisión de certificados bajo proyectos concretos con una/s determinada/s entidad/es. Por este motivo, son unas jerarquías abiertas donde los certificados y la gestión de los mismos se ajustan a las necesidades concretas de un proyecto. En este sentido, y a diferencia de las jerarquías CHAMBERS OF COMMERCE ROOT, los certificados de entidad final emitidos bajo estas jerarquías y sus correspondientes AC y AR no tienen limitación territorial.

Las jerarquías CHAMBERSIGN GLOBAL ROOT organizan la emisión de certificados por AC Subordinadas establecidas en diferentes territorios, mediante AC Subordinadas propiedad de Camerfirma expresamente creadas para la emisión de certificados de AC Subordinadas en dichos territorios, permitiendo adaptarse así de mejor manera a los marcos jurídicos y reglamentarios correspondientes.

Bajo estas jerarquías se permite la emisión de certificados por AC Subordinadas establecidas en cualquier parte del mundo, siempre que las AC y las AR cumplan los requisitos establecidos por Camerfirma, sujetándose en todo caso a la legislación y a la normativa vigentes aplicables.

Las AC Subordinadas que emiten certificados bajo estas jerarquías pueden ser propiedad de Camerfirma o de otros PSC. Todas las AC que operan bajo estas jerarquías lo hacen desde infraestructuras controladas técnicamente por Camerfirma.

Los datos de identificación de los certificados de AC Raíz activas de estas jerarquías son:

- **GLOBAL CHAMBERSIGN ROOT – 2016**

  CN: GLOBAL CHAMBERSIGN ROOT - 2016

  Válido desde (hora UTC): 14/04/2016 07:50:06

  Válido hasta (hora UTC): 08/04/2040 07:50:06

  Número de Serie: 2DD2 2E50 30A6 5E13

  ***X509v3 Subject Key Identifier*:** E89B CD7E 8662 9B7A 4D8C 0097 3985 CF1C 7890 703A

  ***Hash SHA-1*:** 1139 A49E 8484 AAF2 D90D 985E C474 1A65 DD5D 94E2

  ***Hash SHA-256*:** C1D8 0CE4 74A5 1128 B77E 794A 98AA 2D62 A022 5DA3 F419 E5C7 ED73

DFBF 660E 7109

En la tabla siguiente se indica el esquema de AC Raíces y AC Subordinadas activas bajo estas jerarquías, incluyendo, en su caso, los respectivos OID en la extensión *Certificate Policies* de los certificados de cada AC y de los distintos tipos de certificados activos emitidos por cada AC Subordinada bajo esta DPC.

GLOBAL CHAMBERSIGN ROOT – 2016	
AC CAMERFIRMA COLOMBIA – 2016 Emite certificados de AC Subordinadas 2.5.29.32.0 [anyPolicy]	
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001 (AC Subordinada de AC CAMERFIRMA COLOMBIA - 2016) Propiedad de CAMERFIRMA COLOMBIA S.A.S. y regida por sus propias DPC y PC 1.3.6.1.4.1.17326.20.10.0 [Camerfirma]	
CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002 (AC Subordinada de AC CAMERFIRMA COLOMBIA - 2016) Propiedad de CAMERFIRMA COLOMBIA S.A.S. y regida por sus propias DPC y PC 1.3.6.1.4.1.17326.20.10.0 [Camerfirma]	
AC CAMERFIRMA PERÚ – 2016 Emite certificados de AC Subordinadas 2.5.29.32.0 [anyPolicy]	
AC CAMERFIRMA PERÚ CERTIFICADOS – 2016 (AC Subordinada de CAMERFIRMA PERÚ – 2016) Propiedad de CAMERFIRMA PERÚ S.A.C y regida por sus propias DPC y PC 2.5.29.32.0 [anyPolicy]	
AC CAMERFIRMA PERÚ CERTIFICADOS – 2023 (AC Subordinada de CAMERFIRMA PERÚ – 2016) Propiedad de CAMERFIRMA PERÚ S.A.C y regida por sus propias DPC y PC 2.5.29.32.0 [anyPolicy]	
AC bajo esta DPC*	
1.3.6.1.4.1.17326.10.9.8 [Camerfirma]	Certificado No Cualificado OCSP – HSM

*Cada una de las AC indicadas en la tabla, emite su correspondiente certificado OCSP.

A continuación, se describen las AC Subordinadas bajo esta DPC dentro de las jerarquías GLOBAL

CHAMBERSIGN ROOT, y, en su caso, las correspondientes PC de los certificados emitidos activos, excepto la PC de los certificados OCSP (ver sección 1.3.1.5).

1.3.2.2.1 AC CAMERFIRMA COLOMBIA - 2016

Esta AC Subordinada emite certificados de AC Subordinadas dentro del ámbito geográfico de la República de Colombia.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía GLOBAL CHAMBERSIGN ROOT– 2016) son:

CN: AC CAMERFIRMA COLOMBIA - 2016

Válido desde (hora UTC): 14/04/2016 11:10:07

Válido hasta (hora UTC): 09/03/2040 11:10:07

Número de Serie: 3F00 A087 126F 41D2

***X509v3 Subject Key Identifier*:** 8994 7ACB 691B 9E30 5624 C0D4 12BF 5E09 17D7 279C

***Hash SHA-1*:** 394E 613C 7852 7BF4 FF42 3195 9FC4 7ECC 9762 E6E4

***Hash SHA-256*:** 8234 8E56 FF76 5293 EBE7 E2A5 B7B0 57F5 C131 C3BC 68DB E7DB 4353 1F40 C76A 3B2D

1.3.2.2.2 AC CAMERFIRMA PERÚ - 2016

Esta AC Subordinada emite certificados de AC Subordinadas dentro del ámbito geográfico de la República del Perú y más generalmente de los países de LATAM que puedan reconocer su validez.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía GLOBAL CHAMBERSIGN ROOT– 2016) son:

CN: AC CAMERFIRMA PERÚ - 2016

Válido desde (hora UTC): 11/10/2016 08:37:59

Válido hasta (hora UTC): 10/03/2040 08:37:59

Número de Serie: 26F4 AA13 F056 0872

***X509v3 Subject Key Identifier*:** B76A 026D 2CD9 B036 B32B 6C05 AA34 5E06 EDB2 B99B

***Hash SHA-1*:** 45A2 5644 3A16 31C8 51A1 1563 10F5 F385 736B D2C5

***Hash SHA-256*:** 71A0 214D 43E5 B359 6DDB 36AF 8459 E9E5 79AE 929B 800D 94A9 E3F6 71E9 F431 C4F3

1.3.2.3 JERARQUÍA CAMERFIRMA ROOT 2021

Los certificados emitidos bajo esta jerarquía, y sus correspondientes AC y AR no tienen limitación territorial.

Bajo esta jerarquía se permite la emisión de certificados por AC Subordinadas establecidas en cualquier parte del mundo, siempre que las AC y las AR cumplan los requisitos establecidos por Camerfirma, sujetándose en todo caso a la legislación y a la normativa vigentes aplicables.

Las AC Subordinadas que emiten certificados bajo esta jerarquía pueden ser propiedad de Camerfirma o de otros PSC. Todas las AC que operan bajo esta jerarquía lo hacen desde infraestructuras controladas técnicamente por Camerfirma.

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: 3461 2CA9 B6C3 7A12 FE65 50A0 6B28 EEEC EEBA F3E4

***X509v3 Subject Key Identifier*:** 5111 327A 10D0 D88C 4C09 8497 B1A9 3EB2 54BA 87C9

***Hash SHA-1*:** 339F 6EF0 37AA EEBA A0CE 5480 0602 DDFB 186C 1CEE

***Hash SHA-256*:** ADFC 9410 EE0D 1091 EEFD 5CDD FAE5 651E 3B1D 66B6 9C0D ABC5 9E33 91B3 585A 538E

En la CP de cada tipo de certificado se indica el esquema de AC Raíz y AC Subordinadas activas bajo esta jerarquía, incluyendo, en su caso, los respectivos OID en la extensión *Certificate Policies* de los certificados de cada AC y de los distintos tipos de certificados activos emitidos por cada AC Subordinada bajo cada PC.

A continuación, se describen las AC Subordinadas bajo esta DPC dentro de la jerarquía CAMERFIRMA ROOT 2021,.

1.3.2.3.1 AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

Esta AC Subordinada puede emitir certificados cualificados a personas físicas y personas jurídicas (actualmente, solo a personas físicas) dentro de la UE, de acuerdo con los requisitos del Reglamento eIDAS y la Ley 6/2020.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía CAMERFIRMA ROOT 2021) son:

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: 1C20 0D92 1123 B898 380F C2B9 2419 BBA9 9B94 C2C2

***X509v3 Subject Key Identifier*:** C76F 2DC4 108A 6EDD F311 6569 C64A 437B C30F 6814

***Hash SHA-1*:** 2E0F 6F10 E614 5E50 57FC 03B2 53C5 006E E06D 19EE

***Hash SHA-256*:** 4D18 7D4E 5BBA 7BBA D422 B75B EFB4 DCB2 179D 1CCD 115A 18D2 C835 0FFF AC31 6B34

1.3.2.4 *JERARQUÍA INFOCERT-CAMERFIRMA ROOT 2024*

Los certificados emitidos bajo esta jerarquía, y sus correspondientes AC y AR no tienen limitación territorial.

Bajo esta jerarquía se permite la emisión de certificados por AC Subordinadas establecidas en cualquier parte del mundo, siempre que las AC y las AR cumplan los requisitos establecidos por Camerfirma, sujetándose en todo caso a la legislación y a la normativa vigentes aplicables.

Las AC Subordinadas que emiten certificados bajo esta jerarquía pueden ser propiedad de Camerfirma o de otros PSC. Todas las AC que operan bajo esta jerarquía lo hacen desde infraestructuras controladas técnicamente por Camerfirma.

Los datos de identificación de los certificados de AC Raíz activas de estas jerarquías son:

- **INFOCERT-CAMERFIRMA CERTIFICATES 2024**

  CN: INFOCERT-CAMERFIRMA CERTIFICATES 2024

  Válido desde (hora UTC): 22/01/2024 11:55:18

  Válido hasta (hora UTC): 22/01/2045 11:55:18

  Número de Serie: 2E01 DAE2 81C0 16C3 14B3 EEC3 850A F1D8 14FA C663

  ***X509v3 Subject Key Identifier*:** 16A8 FFF5 1905 E947 AAD2 561C 1008 F04D F69A 7359

  ***Hash SHA-1*:** 2E92 F393 1E82 FF9D C65F 4341 6797 A8E2 6ABC 36DA

  ***Hash SHA-256*:** E399 302E 4814 4670 6F9D 9218 BF76 E341 5989 9354 3592 418F 8638 CC08 2CAF E5DC

- **INFOCERT-CAMERFIRMA TIMESTAMP 2024**

  CN: INFOCERT-CAMERFIRMA TIMESTAMP 2024

  Válido desde (hora UTC): 22/01/2024 12:22:31

  Válido hasta (hora UTC): 22/01/2045 12:22:31

  Número de Serie: 40D6 A935 6F81 0EF7 050F 9C94 9EB3 7A83 8849 012A

  ***X509v3 Subject Key Identifier*:** EF53 C938 3002 1F46 0A76 121C EBD3 7820 4097 7D81

  ***Hash SHA-1*:** 75C4 C136 B314 3255 3C9C 0753 06DE ECB5 DDCB 6457

  ***Hash SHA-256*:** 30C7 ABA8 8D1B 2915 BF3A 9AC9 32EB FB8E 61D0 E59D 9592 5569 40E0 0DA2 06F3 B85C

En cada CP se indica el esquema de AC Raíz y AC Subordinadas activas bajo esta jerarquía, incluyendo, en su caso, los respectivos OID en la extensión *Certificate Policies* de los certificados de cada AC y de los distintos tipos de certificados activos emitidos por cada AC Subordinada bajo cada PC.

A continuación, se describen las AC Subordinadas bajo esta DPC dentro de la jerarquía INFOCERT-CAMERFIRMA ROOT 2024.

1.3.2.4.1 INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024

Esta AC Subordinada puede emitir certificados cualificados a personas físicas y personas jurídicas (actualmente, solo a personas físicas) dentro de la UE, de acuerdo con los requisitos del Reglamento eIDAS y la Ley 6/2020.

Los datos de identificación del certificado de esta AC Subordinada (emitido por la AC Raíz de la jerarquía INFOCERT-CAMERFIRMA ROOT 2024) son:

CN: INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024

Válido desde (hora UTC): 16/02/2024 12:55:23

Válido hasta (hora UTC): 16/02/2040 12:55:23

Número de Serie: 3DF7 30E0 DC99 52D7 BFF2 CD30 23D3 745F B203 1452

***X509v3 Subject Key Identifier*:** A9D8 FB35 5AA4 AA49 2F72 3C55 0069 8024 2FCE 20CF

***Hash SHA-1*:** 4C6D 9EFB 188E 7F02 4CD8 776A 743C 551A 1651 FCAD

***Hash SHA-256*:** 8D0B 0805 D9B6 90BD 6E68 459B 56B1 20BE FE88 D6C3 35C5 F229 CA88 6E91 EC90 BBE5

1.3.2.4.2 INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

Estas AC Subordinadas emiten certificados a personas jurídicas para la firma digital de sellos de tiempo.

Los datos de identificación de los certificados de estas AC Subordinadas (emitido por la AC Raíz de la jerarquía INFOCERT-CAMERFIRMA ROOT 2024) son:

CN: INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

Válido desde (hora UTC): 16/02/2024 13:03:17

Válido hasta (hora UTC): 16/02/2040 13:03:17

Número de Serie: 28A4 A018 B3A1 2E20 5AF8 7934 98DE 7A3D 7B21 4C2B

***X509v3 Subject Key Identifier*:** 8D94 321B 4155 0454 423A 2171 E911 9DF5 3480 AB5E

***Hash SHA-1*:** 01BB 36A3 165A 4840 F635 E03B 41FD 11E6 D97E DEB8

***Hash SHA-256*:** F1D4 8530 E034 940B 6553 37A1 B30B 0270 62B4 BA6D 6366 6DAB 1F99 3884

5267 23B3

1.3.2.5 CERTIFICADOS OCSP

Cada AC Raíz y cada AC Subordinada gestionada por Camerfirma dentro de las jerarquías bajo esta DPC emite un certificado OCSP, bajo la correspondiente "PC Certificado No cualificado OCSP", que se utilizará para firmar las respuestas del servicio OCSP de la AC sobre el estado de los certificados emitidos por la AC, mientras la AC esté activa.

Adicionalmente, la AC Subordinada AC CAMERFIRMA FOR NATURAL PERSONS (ver sección 1.3.1.1.1) emite certificados OCSP *default*, bajo la correspondiente "PC Certificado No cualificado OCSP", que se utilizarán para firmar las respuestas de los servicios OCSP de las AC gestionadas por Camerfirma dentro de las jerarquías bajo esta DPC, sobre:

- El estado *unknown* de los certificados emitidos por:
    - Una AC fuera de las jerarquías bajo esta DPC.
    - Una AC no gestionada por Camerfirma dentro de las jerarquías bajo esta DPC.
    - Una AC gestionada por Camerfirma dentro de las jerarquías bajo esta DPC y terminada por un motivo distinto al compromiso de su clave privada (ver sección 5.8.2).
- El estado correspondiente de los certificados emitidos por:
    - Una AC gestionada por Camerfirma dentro de las jerarquías bajo esta DPC y terminada por compromiso de su clave privada (ver sección 5.7.3).

En caso de terminación de la AC Subordinada emisora de los certificados OCSP *default*, estos serán sustituidos por certificados OCSP *default* emitidos, bajo la correspondiente "PC Certificado No cualificado OCSP", por otra AC Subordinada de Camerfirma dentro de la misma jerarquía.

En caso de terminación de la AC Raíz de la jerarquía de los certificados OCSP *default*, estos serán sustituidos por certificados OCSP *default* emitidos, bajo la correspondiente "PC Certificado No cualificado OCSP", por otra AC Subordinada de Camerfirma dentro de otra jerarquía bajo esta DPC.

En caso de cese de actividad de Camerfirma como PSC (ver sección 5.8.1), los servicios OCSP de todas las AC gestionadas por Camerfirma dentro de las jerarquías bajo esta DPC dejarán de estar disponibles en sus direcciones de acceso.

Las claves de los certificados OCSP emitidos, bajo las PC Certificado No cualificado OCSP, por las AC gestionadas por Camerfirma dentro de las jerarquías bajo esta DPC se generan y almacenan en un HSM FIPS 140-2 nivel 3 o CC EAL 4 o superior, No QSCD o QSCD, conforme a los requisitos establecidos en ETSI EN 319 411-1.

1.3.2.6 CERTIFICADOS DE PRUEBAS

Las AC Subordinadas bajo esta DPC pueden emitir certificados con datos ficticios para facilitarlos a

los organismos reguladores, así como a los desarrolladores de aplicaciones para que los utilicen en el proceso de integración o evaluación para la aprobación de los certificados. 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:

DNI	NOMBRE	APELLIDO 1	APELLIDO 2	SEXO
99949990V	NOMDIEZ	ESPECIMENDIEZ	ESPECIMENDIEZ	V
99949991H	NOMUNO	ESPECIMENUNO	ESPECIMENUNO	F
99949992L	NOMDOS	ESPECIMENDOS	ESPECIMENDOS	V
99949993C	NOMTRES	ESPECIMENTRES	ESPECIMENTRES	F
99949994K	NOMCUATRO	ESPECIMENCUATRO	ESPECIMENCUATRO	V
99949995E	NOMCINCO	ESPECIMENCINCO	ESPECIMENCINCO	F
99949996T	NOMSEIS	ESPECIMENSEIS	ESPECIMENSEIS	V
99949997R	NOMSIETE	ESPECIMENSIETE	ESPECIMENSIETE	F
99949998W	NOMOCHO	ESPECIMENOCHO	ESPECIMENOCHO	V
99949999A	NOMNUEVE	ESPECIMENNUEVE	ESPECIMENNUEVE	F

1.3.2.7 AC DE GESTIÓN INTERNA

Camerfirma ha desarrollado una AC de gestión interna, denominada CAMERFIRMA GESTIÓN INTERNA, para la emisión de certificados de operador de AR. Con estos certificados los operadores pueden realizar las acciones propias de su rol en la plataforma de gestión de certificados.

La AC CAMERFIRMA GESTIÓN INTERNA está fuera del alcance de estas DPC y PC.

1.3.3 AUTORIDADES DE REGISTRO (AR)

Una AR puede ser una persona jurídica o una persona física que actúa de acuerdo con esta DPC y, en su caso, mediante un acuerdo suscrito con una AC Subordinada bajo esta DPC (propiedad de Camerfirma), ejerciendo las funciones de gestión de las solicitudes, identificación y registro de los Solicitantes de certificados de entidad final, y, en su caso, de tramitación de solicitudes de revocación y de notificaciones de hechos relacionados con la revocación de certificados de entidad final, y cualquier otra responsabilidad establecida en este documento y en las PC aplicables.

Las AR son autoridades delegadas por las AC Subordinadas, aunque estas son las responsables últimas del servicio.

Bajo esta DPC se reconocen los siguientes tipos de AR:

- **AR Cameral:** gestionada directamente o bajo el control de una Cámara de Comercio, Industria y Navegación española.
- **AR Empresarial:** gestionada por una organización pública o una entidad privada.
- **AR Remota:** AR Empresarial con uso de aplicaciones de terceros ubicadas en una

localización remota que se comunican, mediante integración con una capa de servicios web, con la plataforma de gestión de certificados.

Bajo esta DPC, pueden actuar como AR de las AC Subordinadas:

- La **AC** (Camerfirma).
- **Las Cámaras de Comercio, Industria y Navegación** españolas o las entidades que estas designen.

  Están obligadas a superar las Auditorías exigidas en el contrato con la AC.
- **Empresas españolas**, como entidades delegadas por la AC o por otra AR, a la que se vinculan contractualmente, para realizar la completa identificación y registro del Solicitante y, en su caso, la tramitación de solicitudes de revocación y de notificaciones de hechos relacionados con la revocación, dentro de una determinada organización o demarcación.

  Los operadores de estas AR solo gestionan las solicitudes y los certificados en el ámbito de su organización o demarcación, salvo que se determine de otro modo por la AC o la AR de la que dependen, por ejemplo, los empleados de una corporación, los asociados de una agrupación empresarial o los colegiados de un colegio profesional.

  Están obligadas a superar las Auditorías exigidas en el contrato con la AC.
- **Entidades pertenecientes a las Administraciones Públicas españolas**.

  Están obligadas a superar las Auditorías exigidas en el contrato con la AC.
- **Otras personas jurídicas o agentes, españoles o internacionales, que tengan una relación contractual con la AC.**

  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.

  Están obligadas a superar las Auditorías exigidas en el contrato con la AC.
- **PVP.** Punto de Verificación Presencial que depende siempre de una AR. Puede ser una persona jurídica o una persona física en la que la AR delega parcialmente las tareas de identificación.

  Su principal misión es verificar la identidad del Solicitante mediante personación y comprobación de su documento de identidad y entregar la documentación relativa a la identificación a la AR. Para esas funciones los PVP no están sujetos a formación ni controles.

  En ocasiones, el PVP podrá ver ampliadas sus funciones a las de recogida y cotejo de la documentación presentada por el Solicitante, la comprobación de su adecuación al tipo de certificado solicitado y entrega de esta documentación a la RA de la que depende, pero un PVP nunca puede validar el proceso de registro y decidir la emisión del certificado.

  Un operador de la AR comprueba, según la PC aplicable, la documentación suministrada por el PVP y, en su caso, la documentación presentada directamente a la AR, y, si es correcta, da curso a la emisión del certificado por la AC, sin necesidad de realizar una

nueva identificación del Solicitante.

Habida cuenta de que un PVP no tiene capacidad de registro, se vincula contractualmente con una AR mediante un contrato. 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.

- **PVR.** Punto de Verificación Remota que depende siempre de una AR. Puede ser una persona jurídica o una persona física en la que la AR delega parcialmente las tareas de identificación.

  Su principal misión es identificar al Solicitante mediante procesos de identificación remota por vídeo, que podrán utilizarse para emitir certificados cualificados, siempre y cuando cumplan con las condiciones y requisitos técnicos requeridos por la norma aplicable. Para esas funciones los PVR están sujetos a formaciones y controles específicos.

  En ocasiones, el PVR podrá ver ampliadas sus funciones a las de recepción y cotejo de la documentación presentada por el Solicitante, comprobación de su adecuación al tipo de certificado solicitado y entrega de esta documentación a la RA de la que depende, pero un PVR nunca puede validar el proceso de registro y decidir la emisión del certificado.

  Una vez recibidas las evidencias de la identificación suministradas por el PVR, un operador de la AR comprueba, según la PC aplicable, la documentación suministrada por el PVR y/o, en su caso, la documentación presentada directamente a la AR, y, si es correcta, da curso a la emisión del certificado por la AC, sin necesidad de realizar una nueva identificación del Solicitante.

  Habida cuenta de que un PVR no tiene capacidad de registro, se vincula contractualmente con una AR mediante un contrato. Camerfirma ha elaborado un documento tipo de relación entre la AR y el PVR donde se definen las funciones que la AR delega en el PVR.

1.3.4 SUSCRIPTORES

1.3.4.1 SUSCRIPTORES

Bajo esta DPC, y de acuerdo con el estándar ETSI EN 319 401, el Suscriptor es la persona física o jurídica o la entidad sin personalidad jurídica que ha contratado los servicios de Camerfirma para la emisión de un certificado.

Por tanto, se puede considerar al Suscriptor de un certificado como su propietario.

En cada PC, se define quien puede ser Suscriptor de un certificado

1.3.4.2 TITULAR, FIRMANTE Y CREADOR DE UN SELLO

Bajo esta DPC, y de acuerdo con el estándar ETSI EN 319 411-1, el **Titular** (también conocido como Sujeto) es la entidad identificada en un certificado (en su campo *Subject* y, en su caso, en su extensión *Subject Alternative Name*) como titular de la clave privada asociada con la clave pública contenida en el certificado.

El Firmante, en cuanto persona física Titular del certificado de firma electrónica, será directamente responsable de las obligaciones asociadas al uso y gestión del certificado y de su clave privada asociada.

El Creador de un Sello, en cuanto persona jurídica Titular del certificado de sello electrónico, o en cuanto persona jurídica a la que está vinculada el Titular del certificado de sello electrónico, será directamente responsable de las obligaciones asociadas al uso y gestión del certificado y de su clave privada asociada, sin perjuicio de las obligaciones del Responsable y, en su caso, del Titular.

En esta DPC, el término "Titular/Firmante" se refiere, de forma genérica, al Titular y/o Firmante de los certificados emitidos a personas físicas, y el término "Titular / Creador de un Sello" se refiere, de forma genérica, al Titular y/o al Creador de un Sello de los certificados emitidos a personas jurídicas.

1.3.4.3 SOLICITANTE

Bajo esta DPC, el Solicitante es la persona física que solicita un certificado para sí misma o para la persona jurídica a la que representa.

Durante el proceso de emisión del certificado, se debe identificar al Solicitante conforme a lo establecido en la sección 3.2.3.

1.3.4.4 RESPONSABLE

Bajo esta DPC, el Responsable es la persona física responsable del uso de la clave privada asociada a la clave pública contenida en un certificado.

Durante el proceso de emisión del certificado, el Responsable realiza, entre las siguientes funciones, aquellas que sean aplicables al tipo de dispositivo donde se generan las claves del certificado: entregar la clave pública, recibir la clave privada, definir y/o recibir los datos de activación de la clave privada, recibir el certificado.

1.3.4.5 ENTIDAD

Bajo esta DPC, la Entidad es, en su caso, la organización, de carácter público o privado, individual o colectivo, reconocido en derecho, identificada en los atributos *organizationName* (O) y *organizationIdentifier* del campo *subject* de un certificado, con la que el Titular tiene una determinada vinculación, o que identifica al Titular.

1.3.4.6 PARTES QUE CONFÍAN

En esta DPC , la Parte que Confía es la persona u organización que voluntariamente confía en un certificado emitido por cualquiera de las AC bajo esta DPC.

Las Partes que Confían deben conocer y acatar las limitaciones del uso de los certificados.

1.3.5 OTROS PARTICIPANTES

1.3.5.1 ORGANISMO DE SUPERVISIÓN

El Organismo de Supervisión (también conocido como Organismo de Acreditación) es el órgano competente que admite, acredita y supervisa a los Prestadores de Servicios de Confianza (PSC) dentro de un área geográfica determinada.

El Organismo de Supervisión nacional en el Estado Español es la autoridad competente designada para estas tareas por el Estado Español miembro del Espacio Económico Europeo.

Las AC Subordinadas externas pueden estar sujetas a marcos legales en países o regiones diferentes. En estos casos, la acreditación de la Entidad como PSC cualificado recae en los organismos nacionales correspondientes.

1.3.5.2 OTROS PRESTADORES DE SERVICIOS

Camerfirma podrá utilizar en la prestación de los servicios electrónicos de confianza amparados en esta DPC, los servicios de otros proveedores. La relación de dichos proveedores, así como sus obligaciones, políticas y prácticas aplicables se incluirá en la Política de Certificación específica del servicio de confianza que haga uso de los mismos.

1.4 USOS DEL CERTIFICADO

Los usos apropiados de los certificados se encuentran recogidos en las Políticas de Certificación de Camerfirma para cada tipo de certificados.

1.4.1 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados solo se utilizarán de acuerdo con lo que se establezca en cada Política de Certificación y conforme a la normativa vigente.

1.4.2 USOS PROHIBIDOS DE LOS CERTIFICADOS

Camerfirma incorpora en los certificados información sobre la limitación de uso, bien en las extensiones estándar “Uso de la Clave” (*Key Usage*) y “Restricciones Básicas” (*Basic Constraints*), marcadas como “críticas” en el certificado y, por lo tanto, de cumplimiento obligatorio por parte de las aplicaciones que utilicen el certificado, o bien limitaciones en extensiones estándar como “uso extendido de clave” (*Extended Key Usage*) y “restricciones de nombre” (*Name Constraints*)

y/o mediante textos incorporados el campo “aviso al usuario” (*User Notice*) en la extensión estándar “Políticas de Certificación” (*Certificate Policies*), marcadas como “no críticas” en el certificado, pero de obligado cumplimiento por parte del Titular y de las Partes que Confían.

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso y que vienen descritos en este documento.

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

El uso de los certificados en operaciones que contravienen las PC aplicables a cada uno de los certificados, la DPC, los Términos y Condiciones o los contratos de la AC con las AR o con los Suscriptores tendrá la consideración de uso indebido, a los efectos legales oportunos, eximiéndose por tanto la AC, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realicen los Titulares o cualquier tercero.

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

La clave privada de los certificados es almacenada por Camerfirma únicamente para los certificados en Nube, por lo que, en los otros casos, 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. 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 Jurídico de Camerfirma.

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL 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

AC CAMERFIRMA, S.A.

Dirección: Calle de Rodríguez Marín 88 – 28016 Madrid (España)

Teléfono: +34 91 136 91 05

Email: info@camerfirma.com

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

En cuanto al contenido de esta DPC , 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 certificados emitidos bajo esta DPC, pueden ponerse en contacto con Camerfirma enviando un correo electrónico a la dirección incidentes@camerfirma.com.

1.5.3 PERSONA QUE DETERMINA LA IDONEIDAD DE DPC PARA LA POLÍTICA

El departamento Jurídico de Camerfirma constituye la Autoridad de Políticas (AP) de las jerarquías de la AC descritas anteriormente siendo responsable de la idoneidad de la DPC y las PC.

1.5.4 PROCEDIMIENTOS DE GESTIÓN DEL DOCUMENTO

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

Camerfirma publica cada nueva versión de este documento en su página web https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/. La DPC se publica en formato PDF firmado o sellado electrónicamente con el certificado digital del aprobador.

Esta DPC así como las CP y los Textos Divulgativos (PDS) se revisarán y actualizarán anualmente o cuand se produzcan cambios significativos en la organización o en la normativa aplicable que les afecte.

1.6 DEFINICIONES Y SIGLAS

1.6.1 DEFINICIONES

Autoridad de	Entidad responsable de la emisión y gestión de certificados. Actúa como

Certificación	tercera parte de confianza entre el Titular y la Parte que Confía, asociando una clave pública específica con el Titular. Prestador de Servicios de Confianza que emite certificados.
Autoridad de sellado de tiempo	Prestador de Servicios de Confianza que emite sellos de tiempo usando una o varias unidades de sellado de tiempo.
Autoridad de Políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las PC y DPC.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes, identificación y registro de los Solicitantes de certificados de entidad final, y, en su caso, de tramitación de solicitudes de revocación y de notificaciones de hechos relacionados con la revocación de certificados de entidad final.
Certificación cruzada	Establecimiento de una relación de confianza entre dos AC, mediante la emisión de un certificado por una AC a la otra AC.
Certificado	Archivo que asocia la clave pública con algunos datos del Titular y es firmado por la AC.
Certificado de firma electrónica	Declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.
Certificado cualificado de firma electrónica	Certificado de firma electrónica que ha sido expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el anexo I del Reglamento eIDAS.
Certificado de sello electrónico	Declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona.
Certificado cualificado de sello electrónico	Certificado de sello electrónico que ha sido expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el anexo III del Reglamento eIDAS.
Certificado de AC	Certificado emitido a una AC por otra AC o por la misma AC, cuya clave privada es usada para firmar certificados y/o CRL.
Certificado de entidad final	Certificado emitido a una entidad final por una AC, cuya clave privada no es usada para firmar certificados y/o CRL.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.
Clave privada	Valor matemático usado únicamente por el Titular para la creación de una

	firma digital o el descifrado de datos. También llamada datos de creación de la firma electrónica y datos de creación del sello electrónico.
Creador de un Sello	Persona jurídica identificada en un certificado de sello electrónico. Persona jurídica que crea un sello electrónico.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en una fecha y hora determinada y que es firmada por la AC.
Datos de activación	Datos privados, como los PIN o las contraseñas utilizados para activar la clave privada.
Datos de creación de la firma electrónica	Datos únicos que utiliza el Firmante para crear una firma electrónica. También llamados clave privada.
Datos de creación del sello electrónico	Datos únicos que utiliza el Creador del Sello electrónico para crearlo. También llamados clave privada.
Datos de validación	Datos utilizados para validar una firma electrónica o un sello electrónico. También llamados clave pública.
Declaración de Prácticas de Certificación	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión, gestión, revocación y renovación de certificados.
Dispositivo criptográfico seguro	Dispositivo que almacena la clave privada del usuario, la protege contra cualquier compromiso y realiza funciones de firma y/o descifrado en nombre del usuario.
Dispositivo cualificado de creación de firma electrónica	Dispositivo de creación de firmas electrónica que cumple los requisitos enumerados en el anexo II del Reglamento eIDAS.
Dispositivo cualificado de creación de sello electrónico	Dispositivo de creación de sellos electrónicos que cumple *mutatis mutandis* los requisitos enumerados en el anexo II del Reglamento eIDAS.
Dispositivo de creación de firma electrónica	Equipo o programa informático configurado que se utiliza para crear una firma electrónica.

Dispositivo de creación de sello electrónico	Equipo o programa informático configurado que se utiliza para crear un sello electrónico.
Entidad	Organización, de carácter público o privado, individual o colectivo, reconocido en derecho, identificada en los atributos *organizationName* (O) y *organizationIdentifier* del campo *Subject* de un certificado, con la que el Titular tiene una determinada vinculación, o que identifica al Titular.
Entidad final	Titular de un certificado emitido por una AC, cuya clave privada no es usada para firmar certificados y/o CRL.
Firma electrónica	Datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos, que utiliza el Firmante para firmar.
Firma electrónica avanzada	Firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS: a) estar vinculada al Firmante de manera única; b) permitir la identificación del Firmante; c) haber sido creada utilizando datos de creación de la firma electrónica que el Firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculada con los datos firmados por la misma de forma que cualquier modificación ulterior de los mismos sea detectable.
Firma electrónica cualificada	Firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
Firma digital	Resultado de la transformación de un mensaje, o cualquier tipo de datos, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad); b) que la persona que firma los datos es quien dice ser (identificación); y c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen).
Firma remota	Procedimiento especial de firma electrónica generada por un HSM que garantiza el control exclusivo de la clave privada por el Firmante y que permite la creación de firmas electrónicas a distancia.
Firmante	Persona física identificada en un certificado de firma electrónica. Persona física que crea una firma electrónica.

Hash	Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.
HSM	Dispositivo hardware que genera y protege claves criptográficas, y permite utilizarlas para realizar operaciones criptográficas de modo seguro.
OID	Identificador numérico único registrado bajo la estandarización ISO y que se refiere a un objeto o clase de objeto determinado.
Organismo de Supervisión	Órgano gestor correspondiente que admite, acredita y supervisa a los Prestadores de Servicios de Confianza dentro de un área geográfica determinada.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
Parte que Confía	Persona u organización que voluntariamente confía en un certificado emitido por cualquiera de las AC bajo esta DPC.
PKI	Conjunto de hardware, software, recursos humanos, procedimientos, etc., que componen un sistema usado para la creación y gestión de certificados de clave pública.
Política de Certificación	Conjunto de reglas que definen la aplicabilidad de un certificado a una comunidad y/o un conjunto de aplicaciones o usos con requisitos de seguridad comunes.
Prestador Cualificado de Servicios de Confianza	Prestador de Servicios de Confianza que presta uno o varios servicios de confianza cualificados y al que el Organismo de Supervisión ha concedido la cualificación.
Prestador de Servicios de Confianza	Persona física o jurídica que presta uno o más servicios de confianza, bien como Prestador Cualificado o como Prestador No Cualificado de Servicios de Confianza.
Responsable	Persona física responsable del uso de la clave privada asociada a la clave pública contenida en un certificado.
Sello cualificado de tiempo electrónico	Sello de tiempo electrónico que cumple los requisitos establecidos en artículo 42 del Reglamento eIDAS: a) vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte; b) basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y c) haber sido firmada mediante el uso de una firma electrónica avanzada o

	sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza.
Sello de tiempo electrónico	Datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.
Sello electrónico	Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.
Sello electrónico avanzado	Sello electrónico que cumple los requisitos contemplados en el artículo 36 del Reglamento eIDAS: a) estar vinculado al creador del Sello de manera única; b) permitir la identificación del Creador del sello; c) haber sido creado utilizando datos de creación del sello electrónico que el Creador del Sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y d) estar vinculado con los datos a que se refiere de forma que cualquier modificación ulterior de los mismos sea detectable.
Sello electrónico cualificado	Sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.
Sello remoto	Procedimiento especial de sello electrónico generado por un HSM que garantiza el control de la clave privada por el Creador de un Sello y que permite la creación de sellos electrónicos a distancia.
Servicio de confianza	Servicio electrónico prestado normalmente a cambio de una remuneración, consistente en: a) la expedición de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza; b) la validación de certificados de firma electrónica, certificados de sello electrónico, certificados de autenticación de sitios web o certificados para la prestación de otros servicios de confianza; c) la creación de firmas electrónicas o sellos electrónicos; d) la validación de firmas electrónicas o sellos electrónicos; e) la conservación de firmas electrónicas, sellos electrónicos, certificados de firma electrónica o certificados de sello electrónico; f) la gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia; g) la expedición de declaraciones electrónicas de atributos; h) la validación de declaraciones electrónicas de atributos;

	i) la creación de sellos de tiempo electrónicos; j) la validación de sellos de tiempo electrónicos; k) la prestación de servicios de entrega electrónica certificada; l) la validación de los datos transmitidos a través de servicios de entrega electrónica certificada y las pruebas correspondientes; m) el archivo electrónico de datos y documentos electrónicos; n) la actividad de registro de datos electrónicos en un libro mayor electrónico
Solicitante	Persona física que solicita un certificado para sí misma o para la persona jurídica a la que representa.
Suscriptor	Persona física o jurídica o entidad sin personalidad jurídica vinculada por un acuerdo con Camerfirma, actuando como Prestador de Servicios de Confianza emisor de certificados (Autoridades de Certificación), a cualquier obligación de Suscriptor de uno o varios certificados.
Titular	Entidad identificada en un certificado como titular de la clave privada asociada con la clave pública contenida en el certificado. También llamado Sujeto.
Unidad de sellado de tiempo	Conjunto de hardware y software que es gestionado como una unidad y tiene una única clave de firma de sellos de tiempo activa en un instante de tiempo.

1.6.2 SIGLAS

AAPP	Administraciones Públicas
AC	Autoridad de Certificación
AP	Autoridad de Políticas
AR	Autoridad de Registro
AWS	*Amazon Web Services*. Servicios Web de Amazon.
CAA	*Certification Authority Authorization*. Autorización de AC.
CC	*Common Criteria*. Criterios Comunes.
CN	*Common Name.* Nombre común.
CRL	*Certificate Revocation List*. Lista de certificados revocados.
CSR	*Certificate Signing Request*. Petición de firma de certificado.
DN	*Distinguished Name*. Nombre distintivo.
DNI	Documento Nacional de Identidad

DPC	Declaración de Prácticas de Certificación
EAL	*Evaluation Assurance Level*. Nivel de Garantía de Evaluación.
ECC	*Elliptic Curve Cryptography*
EEE	Espacio Económico Europeo
eIDAS	*electronic IDentification, Authentication and trust Services*
EN	*European Standard*. Estándar Europeo.
ETSI	*European Telecommunications Standards Institute*
FIPS	*Federal Information Processing Standard*
GPS	*Global Positioning System*. Sistema de Posicionamiento Global.
HSM	*Hardware Security Module.* Módulo de Seguridad Hardware.
HTTP	*Hypertext Transfer Protocol*. Protocolo de Transferencia de Hipertexto.
IEC	*International Electrotechnical Commission*. Comisión Electrotécnica Internacional
IETF	*Internet Engineering Task Force*. Grupo de Trabajo de Ingeniería de Internet.
IP	*Internet Protocol*. Protocolo de Internet.
ISO	*International Organization for Standardization*. Organismo Internacional de Estandarización.
ITU	*International Telecommunication Union*. Unión Internacional de Telecomunicación.
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
NCP	*Normalized Certificate Policy*. Política de Certificación Normalizada.
NCP+	*Extended Normalized Certificate Policy*. Política de Certificación Normalizada Extendida.
NIE	Número de Identidad de Extranjero
NIF	Número de Identificación Fiscal
NTP	*Network Time Protocol*
O	*Organization name*. Nombre de la Organización.
OCSP	*Online 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.
PC	Política de Certificación

PDF	*Portable Document Format*
PIN	*Personal Identification Number*. Número de identificación personal.
PKCS	*Public-Key Cryptography Standards*. Estándares de Criptografía de Clave Pública.
PKI	*Public Key Infrastructure*. Infraestructura de Clave Pública.
PCSC	Prestador Cualificado de Servicios de Confianza
PSC	Prestador de Servicios de Confianza
PVP	Punto de Verificación Presencial
PVR	Punto de Verificación Remota
QCP-l	Política de Certificación para Certificados Cualificados en la UE emitidos a personas jurídicas (*legal persons*).
QCP-l-qscd	Política de Certificación para Certificados Cualificados en la UE emitidos a personas jurídicas (*legal persons*) cuando la clave privada y el certificado asociado residen en un QSCD
QCP-n	Política de Certificación para Certificados Cualificados en la UE emitidos a personas físicas (*natural persons*)
QCP-n-qscd	Política de Certificación para Certificados Cualificados en la UE emitidos a personas físicas (*natural persons*) cuando la clave privada y el certificado asociado residen en un QSCD
QSCD	*Qualified electronic Signature/Seal Creation Device*. Dispositivo cualificado de creación de firma electrónica / sello electrónico
RFC	*Request for Comments*
RGPD	Reglamento General de Protección de Datos
ROA	Real Instituto y Observatorio de la Armada
RSA	*Rivest-Shamir-Adleman* (tipo de algoritmo de clave pública)
SHA	*Secure Hash Algorithm*. Algoritmo Seguro de Hash.
SSL	*Secure Sockets Layer* (protocolo de comunicación segura)
TLS	*Transport Layer Security* (protocolo de comunicación segura que sustituye a SSL)
TSA	*Time-Stamping Authority.* Autoridad de sellado de tiempo.
TSL	*Trust-service Status List*. Lista de estados de servicios de confianza.
TSU	*Time-Stamping Unit*. Unidad de sellado de tiempo.
UE	Unión Europea
UTC	*Coordinated Universal Time*. Tiempo universal coordinado.

2 RESPONSABILIDAD DE PUBLICACIÓN Y REPOSITORIOS

2.1 REPOSITORIOS

Los repositorios de Camerfirma para la publicación de la información de certificación están disponibles las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de Camerfirma, Camerfirma realizará los mayores esfuerzos para asegurar que estos repositorios no se encuentren inaccesibles durante más de 24 horas.

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

2.2.1 PRÁCTICAS Y POLÍTICAS DE CERTIFICACIÓN

Camerfirma pone a disposición del público la versión actual de estas DPC y PC en el sitio web con las siguientes direcciones:

- https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/
- https://policy.camerfirma.com
- https://policy2021.camerfirma.com

Una vez publicada una nueva versión de esta DPC y PC, Camerfirma mantendrá a disposición del público la versión anterior en el mismo sitio web, al menos hasta la terminación de todas las AC incluidas en esa versión (ver sección 5.8.2).

2.2.2 TÉRMINOS Y CONDICIONES

El Responsable, y el Titular y/o el Suscriptor si son distintos, reciben información sobre los Términos y Condiciones que deben aceptar antes de la emisión del certificado.

Las Partes que Confían pueden consultar la versión actual de los Términos y Condiciones en el sitio web de Camerfirma:

https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/

2.2.3 DIFUSIÓN DE LOS CERTIFICADOS

Camerfirma pone a disposición del público los certificados de las AC Raíces y Subordinadas propiedad de Camerfirma bajo esta DPC, sus correspondientes certificados OCSP y sus respectivos hashes SHA-1 y SHA-256 en el sitio web:

https://www.camerfirma.com/autoridades-de-certificacion/

Camerfirma seguirá poniendo a disposición del público los certificados de las AC terminadas (ver sección 5.8.2) y sus respectivos hashes SHA-1 y SHA-256 en el mismo sitio web, al menos durante 15 años después de la expiración de todos los certificados emitidos por la AC o hasta el cese de actividad de Camerfirma como PSC (ver sección 5.8.1).

En caso de cese de actividad de Camerfirma como PSC, la provisión de los certificados de las AC de Camerfirma será garantizada por Camerfirma o por una parte confiable a quien transfiera esta obligación, al menos durante 15 años después de la expiración de todos los certificados emitidos por las AC.

Se puede acceder al certificado de una AC a través del protocolo HTTP en la dirección de acceso contenida en la extensión *Authority Information Access* de los certificados emitidos por la AC.

Camerfirma entregará los certificados de entidad final emitidos por las AC Subordinadas bajo esta DPC a sus respectivos Suscriptores, Titulares y Responsables, y, en su caso, de otros PCSC o PSC que gestionan las claves privadas en nombre de los Titulares, de acuerdo con el procedimiento específico de emisión del tipo de certificado.

Camerfirma no entregará los certificados de entidad final emitidos por las AC Subordinadas bajo esta DPC a las Partes que Confían, con excepción de los certificados OCSP y los certificados de TSU propiedad de Camerfirma. Camerfirma pondrá a disposición del público los certificados de TSU propiedad de Camerfirma y de sus correspondientes AC emisoras en el sitio web:

https://www.camerfirma.com/servicios-y-soluciones/sellado-de-tiempo/

Camerfirma sólo pondrá los certificados de AC Subordinadas externas emitidos por las AC Raíces y Subordinadas bajo esta DPC a disposición de las Partes que Confían, en caso de haberlo acordado así con sus respectivas Entidades propietarias.

2.2.4 CRL Y OCSP

Camerfirma pone a disposición del público las CRL de las AC Raíces y Subordinadas propiedad de Camerfirma bajo esta DPC y las direcciones de acceso de sus correspondientes servicios OCSP en el sitio web:

https://www.camerfirma.com/autoridades-de-certificacion/

Camerfirma pondrá a disposición del público las últimas CRL de las AC terminadas (ver sección 5.8.2) y sus respectivos hashes SHA-1 y SHA-256 en el mismo sitio web, al menos durante 15 años después de la expiración de todos los certificados emitidos por la AC o hasta el cese de actividad de Camerfirma como PSC (ver sección 5.8.1).

En caso de cese de actividad de Camerfirma como PSC, la provisión de la información sobre el estado de revocación de los certificados emitidos por las AC de Camerfirma será garantizada por Camerfirma o por una parte confiable a quien transfiera esta obligación, a través de las últimas CRL de las AC, al menos durante 15 años después de la expiración de todos los certificados emitidos por las AC.

Se puede acceder a la/s CRL de una AC a través del protocolo HTTP en las direcciones de acceso contenidas en la extensión *CRL Distribution Points* de los certificados emitidos por la AC.

Se puede acceder al servicio OCSP de una AC a través del protocolo HTTP en la dirección de acceso contenida en la extensión *Authority Information Access* de los certificados emitidos por la AC.

En caso de cese de actividad de Camerfirma como PSC, los servicios OCSP de todas las AC bajo esta DPC dejarán de estar disponibles en sus direcciones de acceso.

El principal servicio de consulta de estado de certificados de las AC bajo esta DPC es el proporcionado por su servicio OCSP.

2.3 FRECUENCIA DE PUBLICACIÓN

Se creará una nueva versión de esta DPC y las PC al menos una vez al año. Camerfirma publica de forma inmediata en su sitio web cualquier nueva versión de estas DPC y las PC.

Las AC bajo esta DPC emiten y publican las CRL con la frecuencia y la máxima latencia especificadas en los apartados 4.9.7 y 4.9.8.

Camerfirma actualizará la información proporcionada por el servicio OCSP de cada AC bajo esta DPC con la máxima latencia especificada en el apartado 4.9.10.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso a los repositorios de Camerfirma para la publicación de la información de certificación es libre y gratuito, excepto:

- Los certificados de entidad final solo estarán a disposición de sus respectivos Suscriptores, Titulares y Responsables, con excepción de los certificados OCSP y los certificados de TSU propiedad de Camerfirma.
- Los certificados de AC Subordinadas externas sólo estarán a disposición de sus respectivas Entidades propietarias, excepto que estas hayan acordado con Camerfirma hacerlos públicos.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 DENOMINACIÓN

3.1.1 TIPOS DE NOMBRES

Los datos del Titular (nombres) se incluyen en el campo *Subject* del certificado, mediante un nombre distintivo (DN, *Distinguished Name*) conforme al estándar de referencia X.500 en ISO/IEC 9594 y, en su caso, en los campos de la extensión *Subject Alternative Name* del certificado.

3.1.2 SIGNIFICADO DE LOS NOMBRES

Todos los DN son significativos, y la identificación de los atributos asociados al Titular es en una forma legible por humanos.

3.1.3 ANONIMATO O PSEUDÓNIMOS DE SUSCRIPTORES

Camerfirma utilizará el seudónimo en aquellos certificados donde se permita en los atributos *CN* y *pseudonym* del DN, guardando confidencialmente la identidad real del Titular/Firmante.

El cálculo del seudónimo se realiza de manera que se identifica unívocamente al auténtico Titular/Firmante.

3.1.4 REGLAS UTILIZADAS PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

Camerfirma atiende en todo caso a lo marcado por el estándar de referencia X.500 en ISO/IEC 9594, los estándares IETF RFC 5280 y RFC 3739 y los estándares ETSI EN 319 412 aplicables.

3.1.5 UNICIDAD DE LOS NOMBRES

Dentro de una misma AC no se pueden volver a asignar los nombres de un Titular que ya hayan sido ocupados a un Titular diferente. Esto se consigue incorporando el identificador fiscal único del Titular en el DN del certificado.

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

Camerfirma no asume ninguna obligación en la emisión de certificados respecto al uso de marcas registradas u otros signos distintivos. Camerfirma no permite deliberadamente el uso de un signo

distintivo sobre el Titular que no ostente derechos de uso. Sin embargo, Camerfirma no está obligada a buscar evidencias acerca de los derechos de uso sobre marcas registradas u otros signos distintivos con anterioridad a la emisión de los certificados.

3.1.7 PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS DE NOMBRES

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

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 MÉTODOS DE PRUEBA DE LA POSESIÓN DE LA CLAVE PRIVADA

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

1) Generación de claves por parte de Camerfirma

   En software: las claves se entregan al Responsable en mano o mediante correo electrónico a través de ficheros protegidos utilizando el Standard PKCS #12. La seguridad del proceso queda garantizada debido a que el código de acceso al fichero PKCS #12 que posibilita la instalación de éste en las aplicaciones, es entregado por un medio distinto al utilizado en la recepción del fichero.

   En QSCD Tarjeta/Token: las claves pueden ser entregadas por Camerfirma al Responsable, directamente o a través de una AR en un dispositivo tarjeta/token criptográfico QSCD, que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS.

   En Tarjeta/Token No QSCD: las claves pueden ser entregadas por Camerfirma al Responsable, directamente o a través de una AR en un dispositivo tarjeta/token criptográfico FIPS 140-2 nivel 3 o CC EAL 4 o superior, No QSCD.

   En QSCD Nube (plataforma centralizada QSCD): Camerfirma utiliza un sistema de almacenamiento remoto de claves, permitiendo al Titular acceder a la clave privada desde diferentes dispositivos. Las claves se almacenan en un HSM QSCD, que permite al Titular/Firmante (o al Titular / Creador de un Sello, en el caso de persona jurídica) utilizar la clave privada bajo su control exclusivo, y que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS.

   En Nube (plataforma centralizada No QSCD): Camerfirma utiliza un sistema de almacenamiento remoto de claves, permitiendo al Titular acceder a la clave privada desde diferentes dispositivos. Las claves se almacenan en un HSM FIPS 140-2 nivel 3 o CC EAL 4 o

superior, No QSCD, que permite al Titular/Firmante (o al Titular/ Creador de un Sello, en el caso de persona jurídica) utilizar la clave privada bajo su control exclusivo (o bajo su control, en el caso de persona jurídica).

2) Generación de las claves por el Titular

El Titular dispone de un mecanismo de generación de claves ya sea software o hardware. Estas claves son generadas en un dispositivo externo no gestionado por Camerfirma u otro PCSC o PSC, por lo que Camerfirma no puede garantizar que dicho dispositivo sea QSCD y por este motivo se cataloga como No QSCD, excepto en el caso de QSCD HSM (certificado de TSU mediante declaración responsable exigida al responsable). La prueba de posesión de la clave privada en estos casos es la petición recibida, que contiene la clave pública, por Camerfirma en formato PKCS #10.

3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN

3.2.2.1 IDENTIDAD

Antes de la emisión de un certificado a una persona jurídica o a una persona física con atributos de vinculación a una Entidad, es necesario comprobar los datos relativos a la constitución y, en su caso, la personalidad jurídica de la Entidad.

Para estos certificados, se exige en todos los casos la identificación de la Entidad, para lo cual la AR, dependiendo de cada caso, requerirá la documentación pertinente en función del tipo de Entidad y/o realizará consultas en las agencias de registro utilizadas para la identificación de las Entidades.

La documentación pertinente en función del tipo de Entidad se encuentra en la página web de Camerfirma, en el apartado informativo del certificado correspondiente.

Para las Administraciones Públicas, no se exige la documentación acreditativa de la existencia de la Administración Pública, órgano, organismo público o entidad de derecho público, dado que esta identidad forma parte del ámbito institucional de la Administración General del Estado o de otras Administraciones Públicas del Estado.

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

Las agencias de registro utilizadas para la identificación de las Entidades son:

- España:
    - Registro Mercantil.
    - Agencia Tributaria.
    - Agencia de registro específica según el tipo de Entidad.

Adicionalmente, para aquellos certificados en los que el Suscriptor es distinto del Titular y, en su

caso, de la Entidad, se exige la identificación del Suscriptor (persona jurídica o entidad sin personalidad jurídica) de la misma forma que para la identificación de la Entidad.

3.2.2.2 MARCAS REGISTRADAS

Ver apartado 3.1.6.

3.2.2.3 VERIFICACIÓN DEL PAÍS

Ver apartado 3.2.2.1.

3.2.2.4 VALIDACIÓN DE LA AUTORIZACIÓN O CONTROL DE DOMINIO

Las AC bajo esta DPC no emiten certificados SSL/TLS.

3.2.2.5 AUTENTICACIÓN DE UNA DIRECCIÓN IP

Las AC bajo esta DPC no emiten certificados SSL/TLS.

3.2.2.6 VALIDACIÓN DEL DOMINIO WILDCARD

Las AC bajo esta DPC no emiten certificados SSL/TLS.

3.2.2.7 EXACTITUD DE LAS FUENTES DE DATOS

Ver apartado 3.2.2.1.

3.2.2.8 REGISTROS CAA

Las AC bajo esta DPC no emiten certificados SSL/TLS y por tanto no hay requisitos sobre los registros de CAA.

3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE

Documento de identidad:

Con carácter previo a la emisión y entrega de un certificado, se exige la comprobación de la identidad del Solicitante, en su caso, presentando el original en vigor de alguno de los siguientes

documentos:

- Nacionalidad española:
  - Documento Nacional de Identidad o Pasaporte.
- Extranjeros de la UE o EEE con NIE:
  - Pasaporte o documento de identidad nacional expedido por un país de la UE o del EEE y Certificado de Número de Identidad de Extranjero (NIE).
- Extranjeros de la UE o EEE sin NIE pero con NIF:
  - Pasaporte o documento de identidad nacional expedido por un país de la UE o del EEE y Certificado de Número de Identificación Fiscal (NIF).
- Extranjeros de la UE o EEE sin NIE ni NIF:
  - Pasaporte o documento de identidad nacional expedido por un país de la UE o del EEE.
- Extranjeros de otros países residentes en España (con NIE):
  - Tarjeta de Residencia o Tarjeta de Identidad de Extranjero con fotografía.
- Extranjeros de otros países no residentes en España (sin NIE) pero con NIF:
  - Pasaporte y Certificado de Número de Identificación Fiscal (NIF).

No se pueden emitir certificados a menores de edad no emancipados, incapacitados judicialmente total o parcial, o cuando existen sospechas fundamentadas de que el Solicitante no está en posesión de sus plenas capacidades mentales.

Se comprueba el control sobre la dirección de correo electrónico incorporada en la solicitud de certificado. Esta comprobación será realizada exclusivamente por la AC, por lo que no se podrá delegar.

Métodos de identificación:

La identidad del Solicitante de un certificado cualificado se comprobará utilizando alguno de los métodos que marca el Reglamento eIDAS y de conformidad con el Derecho nacional aplicable:

1) Personación: se exige la personación del Solicitante ante un operador de la AC, de la AR o del PVP (Punto de Verificación Presencial). El Solicitante puede optar alternativamente por personarse ante un Notario y aportar la solicitud de expedición del certificado con su firma legitimada en presencia notarial.
2) A distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia del Solicitante previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos en el artículo 8 del Reglamento eIDAS con respecto a los niveles de seguridad «alto». Se aceptarán los sistemas de identificación electrónica notificados por los Estados miembros en virtud del artículo 9.1 del Reglamento eIDAS. En el caso de España, se aceptará el DNI electrónico.
3) Por medio de un certificado de una firma electrónica cualificada emitido por una AC de

Camerfirma o de otro PCSC, bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional, o utilizando medios de identificación electrónica conformes a lo indicado en el punto 2, siempre y cuando los datos de identidad del Solicitante estén contenidos en el certificado utilizado.

Si el certificado utilizado también contiene los atributos de vinculación del Solicitante a una Entidad y los datos de identidad de esta Entidad que constarán el certificado solicitado, no se exige lo dispuesto en la sección 3.2.2.1 sobre la comprobación los datos relativos a la constitución y, en su caso, la personalidad jurídica de la Entidad, y lo dispuesto en la sección 3.2.5.1 sobre la presentación de documentación para la comprobación de la vinculación del Solicitante a la Entidad.

4) Otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, de acuerdo con la norma aplicable, en particular las condiciones y requisitos técnicos establecidos en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, modificada por la Orden ETD/743/2022, de 26 de julio.

   Respecto a la identificación del Solicitante, Camerfirma pone a disposición de sus usuarios varios procesos de identificación remota por vídeo, que podrán utilizarse para emitir certificados cualificados. En concreto, los siguientes:

   - Proceso asistido, con la mediación síncrona de un operador.
   - Proceso desasistido, sin necesidad de interacción en línea con un operador, con revisión posterior de un operador.

   En todos los procesos se aplicarán las siguientes medidas adicionales:

   - Si el Solicitante ha presentado un DNI o es titular de un NIE, Camerfirma los datos de identidad del Solicitante, utilizando el número de documento, a través del Servicio de Verificación y Consulta de Datos que el Organismo de Supervisión 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 de protección de datos personales.
   - Por motivos de seguridad y prevención del fraude, sólo se aceptarán documentos de identidad convencionales en este método de identificación (DNI español y pasaportes españoles o extranjeros). La identificación de 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 autoridad de expedición y formación específica.

Lo dispuesto en esta sección sobre la obligación de comprobación de la identidad del Solicitante de un certificado cualificado, así como, en su caso, lo dispuesto en la sección 3.2.2.1 sobre la comprobación los datos relativos a la constitución y, en su caso, la personalidad jurídica de la

Entidad, y lo dispuesto en la sección 3.2.5.1 sobre la vinculación del Solicitante a la Entidad, podrá no ser exigible cuando la identidad u otras circunstancias permanentes del Solicitante constaran ya a Camerfirma o a la AR en virtud de una relación preexistente, en la que, para la identificación del Solicitante, se hubiese empleado el medio señalado en el punto 1) y el período de tiempo transcurrido desde la identificación fuese menor de cinco años.

La identidad del Solicitante de un certificado no cualificado se comprobará utilizando alguno de los métodos de comprobación de la identidad del Solicitante de un certificado cualificado indicados en esta sección, o alguno de los siguientes métodos alternativos:

1) Por medio de un certificado cualificado de una firma electrónica avanzada (firma electrónica cualificada o no cualificada) emitido por una AC de Camerfirma o de otro PCSC, o por medio de un certificado de una firma electrónica avanzada emitido por otra AC en la que la AR o la AC confíe, sin requisitos sobre el método de identificación utilizado para su emisión.
2) Métodos de identificación remota por vídeo no reconocidos a escala nacional.

3.2.4 INFORMACIÓN DE SUSCRIPTOR NO VERIFICADA

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

3.2.5 VALIDACIÓN DE LA AUTORIDAD

3.2.5.1 COMPROBACIÓN DE LA VINCULACIÓN DEL SOLICITANTE Y DEL RESPONSABLE A LA ENTIDAD

Camerfirma deberá verificar la vinculación del solicitante de un certificado de representante legal o de sello de entidad con la empresa u organismo a la que representa, a través de la comprobación de los datos relativos a la extensión y vigencia de las facultades de representación del solicitante.

En las PC se relaciona la documentación requerida para cada tipo de certificado.

Si la documentación aportada por el solicitante se realiza en formato físico, el operador deberá obtener una copia escaneada y almacenarla en sus ficheros informáticos.

3.2.5.2 IDENTIDAD DEL SERVICIO O MÁQUINA

Las AC bajo esta DPC no emiten certificados SSL/TLS.

3.2.5.3 CONSIDERACIONES ESPECIALES PARA LA EMISIÓN DE CERTIFICADOS FUERA DE

TERRITORIO ESPAÑOL

La documentación requerida para ello es la que legalmente procede en cada país siempre y cuando permita cumplir con la obligación de identificación correspondiente de acuerdo con la legislación española.

3.2.6 CRITERIOS PARA LA INTEROPERACIÓN

Camerfirma puede proporcionar servicios que permitan que otra AC 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 AC; para lo cual, deben establecerse contractualmente los términos y criterios correspondientes.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN CON CAMBIO DE CLAVES

La renovación de un certificado con cambio de claves es el proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado antes de su expiración, cuando su fecha de expiración está próxima o cuando deba ser sustituido (sin modificación de los datos esenciales).

Un certificado no puede ser renovado después de su fecha de caducidad, y en su lugar se debe realizar una nueva emisión del certificado.

Para los certificados de sello electrónico, de firma de código, de TSU, de AC y OCSP no se realizan renovaciones, sino que se realizan nuevas emisiones de certificados.

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN DE UNA SOLICITUD DE RENOVACIÓN CON CAMBIO DE CLAVES RUTINARIA

La identificación y autenticación de una solicitud de renovación con cambio de claves se realiza mediante el certificado válido a renovar o en base a una relación preexistente.

En ambos casos, los datos del Titular/Firmante en el certificado no deben haber cambiado (EXCEPCIÓN: en los casos de renovación de un certificado cuando su fecha de expiración está próxima y en algunos casos de sustitución de un certificado, se permite cambiar la dirección de email contenida en el certificado) y, en el caso de un certificado cualificado, la identificación del Titular/Firmante debe haberse realizado de forma presencial den un periodo de tiempo menor a cinco años. Si esto no se cumple, se debe realizar una nueva identificación y emisión del certificado.

3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN DE UNA SOLICITUD DE RENOVACIÓN CON CAMBIO DE CLAVES DESPUÉS DE LA REVOCACIÓN

Una vez que un certificado ha sido revocado, no se puede renovar, y en su lugar se debe realizar una nueva emisión del certificado.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE UNA SOLICITUD DE REVOCACIÓN

La identificación y autenticación de una solicitud de revocación o suspensión o de una notificación de hechos que pueden indicar la necesidad de revocación de certificados se realiza, para cada uno de los procedimientos disponibles para los distintos tipos de certificados, conforme a lo establecido en la sección 4.9.3.

Camerfirma, o cualquiera de sus AR, puede, por iniciativa propia, solicitar la revocación o la suspensión de un certificado si:

- tiene conocimiento o sospecha de que la clave privada del Titular ha sido comprometida,
- o tiene conocimiento o sospecha de cualquier otro evento que aconseje tomar dicha medida.

4 REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

Camerfirma emplea sus plataformas para la gestión del ciclo de vida de los certificados de entidad final bajo esta DPC y las PC.

Estas plataformas permiten realizar las acciones relativas a la solicitud, el procesamiento de la solicitud, la emisión, la aceptación, la renovación, la revocación y la suspensión de los certificados de entidad final.

Los servicios de estas plataformas están disponibles las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de Camerfirma, Camerfirma realizará los mayores esfuerzos para asegurar que estos servicios no se encuentren inaccesibles durante más de 24 horas.

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Una solicitud de certificado puede ser presentada por el Solicitante, con participación, en su caso, del Responsable, y/o del Titular, y/o del Suscriptor o la Entidad.

4.1.2 PROCESO DE SOLICITUD DE CERTIFICADOS Y RESPONSABILIDADES

4.1.2.1 FORMULARIOS WEB

Las solicitudes de los certificados se realizan de forma general mediante el acceso a los formularios de solicitud en la página web de Camerfirma, o mediante el envío al Solicitante o al Responsable de un enlace a un formulario concreto.

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

El formulario permitirá la incorporación de un CSR (PKCS #10) en caso de que el Titular haya creado las claves en un dispositivo externo no gestionado por Camerfirma.

El Responsable, y el Titular si son distintos, reciben, después de la confirmación de los datos de solicitud, un correo electrónico en la cuenta asociada a la solicitud del certificado un enlace para confirmar la solicitud y aceptar los Términos y Condiciones.

Una vez confirmada la solicitud, el Solicitante es informado de la documentación que debe presentar en una oficina de registro habilitada y cumplir con el requisito de identificación

presencial si esta es pertinente.

Las solicitudes de certificados de AC Subordinada y TSU deben realizarse formalmente a través de la solicitud de una oferta comercial y, en el caso de certificados de TSU, posteriormente incorporadas en los formularios de solicitud.

Existen procedimientos especiales donde el operador de registro entrega al Solicitante o al Responsable las condiciones de uso en papel o mediante correo electrónico.

4.1.2.2 LOTES

Las plataformas permiten igualmente circuitos de solicitud mediante lotes. En este caso, el Suscriptor o la Entidad enviará a la AR un fichero estructurado según un diseño prefijado por Camerfirma con los datos de los Titulares.

4.1.2.3 SOLICITUDES DE CERTIFICADOS DE TSU Y AC SUBORDINADA EXTERNAS

Las solicitudes para la emisión de certificados de TSU o AC Subordinada externa se realizarán mediante una petición de oferta comercial a través de equipo.comercial@camerfirma.com.

Camerfirma se reserva el derecho a enviar un auditor interno o externo para comprobar que el desarrollo de la ceremonia de creación de claves cumple los requisitos de la correspondiente PC de TSU, o los requisitos de AC Subordinada bajo la correspondiente AC emisora en esta DPC.

Cuando el cliente genere por sus propios medios las claves criptográficas en un dispositivo HSM, Camerfirma recopilará las evidencias necesarias, para lo cual solicitará un acta firmada de ceremonia de generación de las claves, conforme a los requisitos establecidos en ETSI EN 319 421 (certificados de TSU) o ETSI EN 319 411-1 (certificados de AC Subordinada), indicando al menos lo siguiente:

- El procedimiento seguido para la generación de las claves.
- Las personas implicadas.
- Fecha de inicio y fin de la ceremonia.
- El entorno en el que se ha realizado.
- El HSM utilizado (marca y modelo).
- En su caso, la configuración del HSM para ser operado conforme a FIPS 140-2 nivel 3 o FIPS 140-3 nivel 3 o CC EAL 4 o superior.
- Política de seguridad empleada: tamaño de claves, parámetros de generación de las claves, exportable/no exportable y cualquier dato relevante adicional.
- La petición PKCS #10 generada, o su hash.
- Incidencias presentadas y su resolución.

Esta acta se incorporará por parte de la AC emisora al expediente documental soporte para la

emisión del certificado.

4.1.2.4 SOLICITUDES VÍA CAPA DE SERVICIOS WEB (WS)

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

Antes de iniciar la emisión mediante este sistema se debe contar con un informe técnico favorable de Camerfirma, un contrato donde la AR se compromete a mantener el sistema en condiciones de seguridad óptimas y a notificar a Camerfirma cualquier modificación o incidencia. Adicionalmente se deben presentar auditorías donde se comprueben:

1) Expedientes documentales de los certificados emitidos.
2) Que los certificados están siendo emitidos bajo las directrices marcadas por esta DPC y por las PC aplicables bajo las que se rigen.

4.1.2.5 PETICIÓN DE CERTIFICACIÓN CRUZADA

Camerfirma permite bajo estas prácticas la certificación cruzada.

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

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

4.2 PROCESAMIENTO DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Para los certificados de entidad final:

- Una vez haya tenido lugar una petición de certificado, el operador de la AR mediante el acceso a las plataformas de gestión de certificados verifica que la información proporcionada es conforme.
- El operador de la AR accede de forma segura a la plataforma tras superar un proceso de formación y evaluación.
- Es necesaria la autenticación multifactor para el acceso a las plataformas de gestión de certificados.

Para certificados de AC Subordinada:

- Mediante aceptación comercial correspondiente a la solicitud de un cliente.

4.2.2 APROBACIÓN O RECHAZO DE LA SOLICITUD

Para los certificados de entidad final:

- El operador de la AR visualiza las peticiones pendientes de tramitar y que le han sido asignadas.
- El operador de la AR queda a la espera de que el Titular/Firmante entregue la documentación correspondiente.
- En las solicitudes vía capa de WS la petición viene autenticada en origen aprobándose la emisión del certificado por parte de la plataforma cuando el origen y la autenticación es correcta.
- Si la información no es correcta, la AR deniega la petición. En caso de que los datos se verifiquen correctamente la Entidad de Registro aprobará la emisión del certificado.

Para certificados de AC Subordinada:

- Mediante aceptación comercial correspondiente a la solicitud de un cliente.

4.2.3 PLAZO PARA RESOLVER LA SOLICITUD

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

Las solicitudes presentadas a través de las plataformas se validan una vez comprobada la identidad del Solicitante y la documentación acreditativa asociada al perfil del certificado. Camerfirma procederá siempre que sea viable a eliminar las solicitudes que lleven más de 1 año sin ser atendidas.

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

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE LA AC DURANTE EL PROCESO DE EMISIÓN

4.3.1.1 CERTIFICADOS EN SOFTWARE

Una vez aprobada la solicitud, el Responsable recibe un correo electrónico con la notificación de

este hecho y procede a la generación y descarga del certificado. El usuario deberá custodiar el PIN de instalación y el código de revocación de sus certificados.

4.3.1.2 CERTIFICADOS EN TARJETA/TOKEN (QSCD O NO QSCD)

El Responsable dispone de un dispositivo criptográfico donde se almacenarán las claves y el certificado.

En el caso de que la carga del certificado la realice directamente la AR. El operador de la AR elegirá sobre qué tipo de tarjeta o token criptográfico quiere realizar la generación de las claves, para lo cual la estación de trabajo del operador de la AR estará configurada adecuadamente con el CSP (*Cryptographic Service Provider*) correspondiente. Actualmente Camerfirma admite varios tipos de tarjetas y tokens USB (QSCD y No QSCD). Si la carga del certificado la realiza el responsable, deberá igualmente estar configurado el CSP y seguir las instrucciones de descarga.

Para las tarjetas proporcionadas por Camerfirma el Responsable recibirá en la cuenta de correo electrónico asociada, el código de acceso al dispositivo criptográfico y el código de desbloqueo, así como un PIN de revocación. Para el resto de las tarjetas la gestión de PIN/PUK está fuera del alcance de este documento.

4.3.1.3 CERTIFICADOS EMITIDOS MEDIANTE SOLICITUDES VÍA SERVICIOS WEB

Las solicitudes pueden ser recibidas mediante llamadas convenientemente autenticadas desde los servicios WS de las plataformas según apartado 4.1.2.4.

4.3.1.4 CERTIFICADOS EN NUBE (QSCD O NO QSCD)

Una vez aprobada la solicitud, el Responsable recibe un correo electrónico con la notificación de este hecho y cómo proceder a la generación y descarga del certificado en la nube.

Si el dispositivo está certificado como dispositivo cualificado de creación de firma o de creación de sello (QSCD), el certificado se emite con los OID que permitirán identificarlo como un certificado emitido en un dispositivo QSCD.

Si por el contrario, el dispositivo no está certificado como dispositivo cualificado de creación de firma o de creación de sello (QSCD), el certificado no contendrá los OID que permitirían identificarlo como un certificado emitido en un dispositivo QSCD.

4.3.2 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO AL SUSCRIPTOR

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

Los certificados de AC Subordinada se emiten bajo la ejecución de una ceremonia de claves y son posteriormente entregados al Responsable.

4.4 ACEPTACIÓN DE CERTIFICADOS

4.4.1 CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DEL CERTIFICADO

Una vez entregado o descargado el certificado, el Titular dispone de un periodo de 14 días naturales para comprobar su correcta emisión (determinar si los datos son correctos y corresponden con la realidad), una vez sobrepasado este periodo se considera aceptado el certificado emitido.

Aceptando el certificado, se confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AC o cualquier tercero que de buena fe confíe en el contenido del certificado.

Si el certificado no ha sido emitido correctamente por causas técnicas o por existir alguna diferencia entre los datos suministrados y el contenido del certificado, ello deberá ser comunicado de inmediato a la AC para que proceda a su revocación y a la emisión de un nuevo certificado. La AC entregará un nuevo certificado sin coste en caso de que la diferencia entre los datos sea causada por un error no imputable al usuario.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA AC

Una vez entregado o descargado el certificado de entidad final, se inscribirá en el registro de certificados interno y la AC no lo hará público, con excepción de los certificados OCSP y los certificados de TSU propiedad de Camerfirma (ver sección 2.2.3).

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS ENTIDADES

Los certificados de las TSU de Camerfirma que emiten sellos cualificados de tiempo electrónicos se notifican al Organismo de Supervisión nacional para su incorporación en la TSL.

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

Los certificados de las AC Subordinadas de Camerfirma que emiten certificados cualificados se notifican al Organismo de Supervisión nacional para su incorporación en la TSL.

En su caso, los certificados de las AC Raíces y las AC Subordinadas se notifican a un repositorio de información gestionado por Mozilla, que incorpora información sobre Autoridades de Certificación – CCADB. Esta base de datos es utilizada por diversos programas comerciales para gestionar sus almacenes de confianza.

4.5 USO DEL PAR DE CLAVES Y LOS CERTIFICADOS

4.5.1 USO DEL CERTIFICADO Y LA CLAVE PRIVADA DEL SUSCRIPTOR

Los certificados de Camerfirma solo podrán ser utilizados para los usos establecidos en esta DPC y en las PC de cada tipo de certificado.

La limitación de uso de la clave viene definida en el contenido del certificado en las extensiones: *Key Usage*, *Extended Key Usage* y *Basic Constraints*.

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA

Las Partes que Confían deben usar la clave pública y el certificado según lo estipulado en estas DPC y en las PC y según lo indicado en los Términos y Condiciones.

Las Partes que Confían deben estar familiarizadas con el ámbito de uso del certificado tal y como se indica en esta DPC y las PC y en el propio certificado. También deben confirmar la validez de un certificado antes de utilizar la clave pública contenida en él, asegurándose 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.

4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

No se permite la renovación de certificados sin cambio de claves.

4.6.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

No estipulado.

4.6.2 QUIÉN PUEDE SOLICITAR LA RENOVACIÓN SIN CAMBIO DE CLAVES

No estipulado.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

No estipulado.

4.6.4 NOTIFICACIÓN DE LA EMISIÓN DEL NUEVO CERTIFICADO AL SUSCRIPTOR SIN CAMBIO DE CLAVES

No estipulado.

4.6.5 CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DEL CERTIFICADO RENOVADO SIN CAMBIO DE CLAVES

No estipulado.

4.6.6 PUBLICACIÓN DEL CERTIFICADO RENOVADO SIN CAMBIO DE CLAVES POR LA AC

No estipulado.

4.6.7 NOTIFICACIÓN DE LA EMISIÓN DE CERTIFICADO RENOVADO SIN CAMBIO DE CLAVES POR LA AC A OTRAS ENTIDADES

No estipulado.

4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

La renovación de un certificado con cambio de claves es el proceso que debe realizarse para obtener un nuevo par de claves y un nuevo certificado antes de su expiración, cuando su fecha de expiración esté próxima o cuando deba ser sustituido (sin modificación de datos del Titular).

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

4.7.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

En los casos permitidos, un certificado puede ser renovado con cambio de claves antes de su fecha de caducidad.

No se permite la renovación de certificados para:

- Certificados de sello electrónico y de firma de código. Se deben realizar nuevas emisiones de los certificados.
- Certificados de TSU. Se realizan nuevas emisiones de los certificados, antes de que quede 1 año para su fecha de caducidad.
- Certificados de AC Raíz y AC Subordinada. Se realizan nuevas emisiones de los certificados en un procedimiento nuevo en base a una planificación previa, mediante ceremonia elaborada al efecto, controlando que el tiempo de vida del certificado siempre sea superior

al máximo tiempo de validez de los certificados que se emiten bajo su rama jerárquica. Ver sección 5.6.

- Certificados OCSP. Se realizan nuevas emisiones de los certificados periódicamente, antes de su fecha de caducidad.

En los siguientes casos no se permite la renovación de un certificado, y en su lugar se debe realizar una nueva emisión del certificado:

- El certificado ha caducado.
- El certificado ha sido revocado.
- Los datos del Titular/Firmante en el certificado han cambiado. EXCEPCIÓN: en los casos de renovación de un certificado cuando su fecha de expiración está próxima y en algunos casos de sustitución de un certificado, se permite cambiar la dirección de email contenida en el certificado.
- En el caso de un certificado cualificado, si han trascurrido más de 4 años desde la última identificación fehaciente del Solicitante.

4.7.2 QUIÉN PUEDE SOLICITAR LA RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

La renovación de un certificado con cambio de claves puede ser solicitada por:

- El Titular/Firmante, cuando la fecha de expiración del certificado está próxima y en algunos casos de sustitución del certificado (sin modificación de datos del Titular/Firmante).
- La AR a través de la cual se emitió el certificado, en algunos casos de sustitución del certificado (sin modificación de datos del Titular/Firmante).
- La AC (Camerfirma), en algunos casos de sustitución del certificado (sin modificación de datos del Titular/Firmante).

4.7.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Antes de renovar un certificado con cambio de claves, se comprueba que los datos del Titular/Firmante en el certificado no han cambiado. Si cualquier dato del Titular/Firmante en el certificado ha cambiado, se debe realizar el proceso de una nueva emisión y, en su caso, se debe revocar el certificado antiguo. EXCEPCIÓN: en los casos de renovación de un certificado, se permite cambiar la dirección de email contenida en el certificado.

En el caso de renovación de certificados cualificados, se permite la emisión del certificado sin realizar una identificación presencial del Titular/Firmante durante un periodo de 4 años desde su última identificación presencial. Una vez han trascurrido los 4 años, el Titular/Firmante deberá realizar el proceso de una nueva emisión.

El proceso técnico de emisión del certificado en la renovación con cambio de claves es igual al que

se sigue cuando se realiza una nueva emisión.

El proceso de renovación de un certificado cuando su fecha de expiración está próxima se inicia a partir del correo electrónico de aviso de caducidad o directamente a través del siguiente sitio web de Camerfirma:

https://www.camerfirma.com/ayuda/utilidades/renovacion-de-certificados/

Este proceso requiere usar la clave privada asociada al certificado válido a renovar.

- Una vez identificado con el certificado a renovar, el aplicativo presenta al Titular/Firmante los datos contenidos en el certificado antiguo y le pide la confirmación de dichos datos. Si algún dato del Titular/Firmante contenido en el certificado ha cambiado, se debe realizar el proceso de una nueva emisión y, en su caso, se debe revocar el certificado antiguo. EXCEPCIÓN: el aplicativo permite al Titular/Firmante modificar la dirección de email asignada al certificado.
- La petición se registra en el aplicativo de AR donde el operador, una vez revisados los datos, procede a pedir la emisión del certificado a la AC.

En algunos casos de sustitución de un certificado, el proceso de renovación se inicia a partir de un correo electrónico enviado al Titular/Firmante. Este proceso requiere usar la clave privada asociada al certificado válido a renovar.

- Una vez identificado con el certificado a renovar, el aplicativo presenta al Titular/Firmante los datos contenidos en el certificado antiguo y le pide la confirmación de dichos datos. Si algún dato del Titular/Firmante contenido en el certificado ha cambiado, se debe realizar el proceso de una nueva emisión y, en su caso, se debe revocar el certificado antiguo. EXCEPCIÓN: en algunos casos de sustitución de un certificado, el aplicativo permite al Titular/Firmante modificar la dirección de email asignada al certificado.
- La petición se registra en el aplicativo de AR donde el operador, una vez revisados los datos, procede a pedir la emisión del certificado a la AC.
- La AC emite el nuevo certificado tomando como inicio de su validez el mismo momento de renovación.
- Posteriormente, en su caso, se revoca el certificado antiguo.

En otros casos de sustitución de un certificado, el proceso de renovación es realizado por un operador de la AR a través de la cual se emitió el certificado o por un operador de la AC. Este proceso no requiere usar la clave privada asociada al certificado válido a renovar.

- La petición se registra en el aplicativo de AR donde el operador, una vez revisados los datos, procede a pedir la emisión del certificado a la AC. Si algún dato del Titular/Firmante contenido en el certificado ha cambiado, se debe realizar el proceso de una nueva emisión y, en su caso, se debe revocar el certificado antiguo.
- La AC emite el nuevo certificado tomando como inicio de su validez el mismo momento de renovación.
- Posteriormente, en su caso, se revoca el certificado antiguo.

4.7.4 NOTIFICACIÓN DE LA EMISIÓN DEL NUEVO CERTIFICADO CON CAMBIO DE CLAVES AL SUSCRIPTOR

Según lo establecido en la sección 4.3.2.

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

Según lo establecido en la sección 4.4.1.

4.7.6 PUBLICACIÓN DEL CERTIFICADO RENOVADO CON CAMBIO DE CLAVES POR LA AC

Según lo establecido en la sección 4.4.2.

4.7.7 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO RENOVADO CON CAMBIO DE CLAVES POR LA AC A OTRAS ENTIDADES

Según lo establecido en la sección 4.4.3.

4.8 MODIFICACIÓN DE CERTIFICADOS

Cualquier necesidad de modificación de datos del Titular en un certificado requiere una nueva solicitud de certificado. Se realizará la emisión de un nuevo certificado con nuevas claves y los datos corregidos y, en su caso, se revocará el certificado antiguo.

EXCEPCIÓN: en casos muy específicos de certificados de AC o de TSU (por ejemplo, en caso de cambio del algoritmo de hash de firma del certificado), se puede permitir que el nuevo certificado tenga las mismas claves que el certificado antiguo, siempre y cuando el fin del periodo de validez del nuevo certificado no sea superior al fin del periodo de validez del antiguo certificado.

4.8.1 CIRCUNSTANCIAS PARA LA MODIFICACIÓN DEL CERTIFICADO

No estipulado.

4.8.2 QUIÉN PUEDE SOLICITAR LA MODIFICACIÓN DEL CERTIFICADO

No estipulado.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DE CERTIFICADOS

No estipulado.

4.8.4 NOTIFICACIÓN DE LA EMISIÓN DEL NUEVO CERTIFICADO AL SUSCRIPTOR

No estipulado.

4.8.5 CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No estipulado.

4.8.6 PUBLICACIÓN DEL CERTIFICADO MODIFICADO POR LA AC

No estipulado.

4.8.7 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS ENTIDADES

No estipulado.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

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

Si un certificado es revocado, queda invalidado antes de su fecha y hora de caducidad. Cualquier firma realizada con él después de que su revocación se haga efectiva queda invalidada.

La revocación de un certificado es definitiva y, por tanto, irreversible.

La suspensión, por su parte, supone una revocación con motivo de suspensión (es decir, un caso particular de revocación). En este caso, se revoca un certificado de forma preventiva hasta que se decida su revocación definitiva o su reactivación.

La revocación o suspensión de un certificado se hace efectiva desde el momento en que se incluya en los servicios de comprobación del estado de los certificados de la AC emisora (publicación de la CRL o servicio OCSP).

Los certificados revocados o suspendidos no pueden ser utilizados bajo estas DPC y PC.

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Un certificado será revocado debido a:

Circunstancias generales que afectan a la información contenida en el certificado:

- Descubrimiento de que alguno de los datos aportados en la solicitud del certificado y que consten en él es incorrecto o incompleto.
- Descubrimiento de que algún otro dato contenido en el certificado es incorrecto o incompleto.
- Alteración posterior de las circunstancias verificadas para la expedición del certificado y que consten en él.
- Modificación de cualquier otro dato contenido en el certificado.

Circunstancias que afectan la seguridad de la clave privada o del certificado:

- Compromiso de la clave privada o de la infraestructura o sistemas de la AC que emitió el certificado, siempre que este incidente afecte a la fiabilidad de los certificados emitidos.
- Infracción por la AC o la AR de los requisitos previstos en los procedimientos de gestión de certificados establecidos en estas DPC y PC.
- Compromiso o sospecha de compromiso de la seguridad de la clave privada o del certificado, incluido en caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.
- Acceso o uso no autorizado por un tercero a/de la clave privada del certificado.
- Falta de diligencia en la custodia de la clave privada por el Titular o por el Responsable.
- Mal uso del certificado por el Titular o por el Responsable.

Circunstancias que afectan la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Pérdida de los datos de activación de la clave privada en el dispositivo criptográfico.
- Acceso no autorizado por un tercero a los datos de activación de la clave privada en el dispositivo criptográfico.
- Falta de diligencia en la custodia del dispositivo criptográfico y/o de los datos de activación de la clave privada en el dispositivo criptográfico.
- Incumplimiento por el Titular o por el Responsable de las normas de uso del dispositivo criptográfico establecidas en esta DPC y las PC o en los Términos y Condiciones.

Circunstancias que afectan al Suscriptor, al Titular, al Solicitante, al Responsable o a la Entidad:

- Finalización de la relación entre la AC y el Suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al Titular.

- Infracción por el Suscriptor, el Titular, el Solicitante, el Responsable o la Entidad de los requisitos establecidos para solicitar el certificado.
- Infracción por el Suscriptor, el Titular, el Solicitante, el Responsable o la Entidad de parte de sus obligaciones, responsabilidades y garantías establecidas en estas DPC y PC o en los Términos y Condiciones.
- Capacidad modificada judicialmente o incapacidad sobrevenida, total o parcial, o fallecimiento del Titular/Firmante.
- Extinción de la personalidad jurídica de la Entidad o disolución de la Entidad sin personalidad jurídica.
- Indicación por el Suscriptor de que la solicitud del certificado no fue autorizada y de que no concede la autorización con carácter retroactivo.
- Cancelación o expiración de la autorización del Suscriptor al Titular.
- En el caso de los certificados emitidos a personas jurídicas, cancelación de la autorización del Suscriptor al Responsable o finalización de la relación entre el Titular y el Responsable, cuando el Responsable todavía tiene, o se sospeche que tiene, acceso a la clave privada.
- Revocación solicitada por el Titular, el Suscriptor, la Entidad, o un tercero autorizado.
- Solicitud realizada por el Solicitante, el Titular/Firmante o el Responsable para la modificación o eliminación de sus datos personales de los registros de Camerfirma.

Circunstancias que afectan al cumplimiento de la normativa aplicable:

- El certificado fue emitido con incumplimiento de los requisitos establecidos en la versión de estas DPC y PC y/o de los Términos y Condiciones vigentes en el momento de emisión del certificado.
- El certificado fue emitido con incumplimiento de los requisitos establecidos en la normativa legal y/o en la versión de los estándares ETSI aplicables (ver sección 1.1) vigentes en el momento de emisión del certificado.
- El certificado ha dejado de cumplir los requisitos establecidos en la versión de estas DPC y PC y/o de los Términos y Condiciones, y/o en la normativa legal y/o en la versión de los estándares ETSI aplicables vigentes en el momento de emisión del certificado, por alteración posterior de las circunstancias verificadas para la expedición del certificado, por ejemplo, porque el dispositivo criptográfico ha dejado de estar certificado como dispositivo cualificado de creación de firma o de creación de sello (QSCD) y el certificado contiene el correspondiente *QCStatement* en la extensión *Qualified Certificate Statements*.

Otras circunstancias:

- Falta de pago del certificado.
- Resolución firme de la autoridad administrativa o judicial competente.
- Suspensión del certificado por un periodo superior al establecido en estas DPC y PC (ver sección 4.9.16).

- Cese de actividad de Camerfirma como PSC (ver sección 5.8.1).
- Terminación de la AC (ver sección 5.8.2).
- En su caso, terminación de la AR (ver sección 5.8.3).
- Cualquier otra circunstancia especificada en estas DPC y PC o en los Términos y Condiciones.
- Cualquier otra circunstancia especificada en la normativa legal y/o en los estándares ETSI aplicables (ver sección 1.1).

El proceso de revocación no se aplica a certificados de AC Raíz.

4.9.2 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

La revocación de un certificado puede ser solicitada por:

- El Responsable.
- El Titular.
- El Suscriptor.
- La Entidad.
- Un tercero autorizado.
- La AR a través de la cual se emitió el certificado.
- La AC (Camerfirma).

Cualquier persona interesada puede notificar a la AR o a la AC hechos que pueden indicar la necesidad de revocación de un certificado.

4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La revocación de un certificado puede ser solicitada mediante alguno de los siguientes procedimientos:

1) Servicio de revocación en línea.

   Este procedimiento está disponible para todos los tipos de certificados de entidad final, excepto los certificados de TSU y OCSP.

   La revocación será solicitada a través del servicio de revocación en línea localizado en el siguiente sitio web de Camerfirma, introduciendo el PIN de revocación del certificado y la dirección de email en la que se ha entregado, y seleccionando el motivo de revocación:

   https://www.camerfirma.com/ayuda/utilidades/revocacion-de-certificados/

   El PIN de revocación del certificado inicial es entregado al Responsable en su dirección de email declarada en el formulario de solicitud del certificado, durante el proceso de emisión del certificado.

En caso de que el Titular lo solicite, se reenviará el PIN de revocación del certificado al Titular en su dirección de email declarada en el formulario de solicitud del certificado.

El solicitante de la revocación podrá ser el Responsable, el Titular, o cualquiera de los otros contemplados en la sección 4.9.2, si, conforme a lo acordado entre ellos, el Responsable o el Titular les comunica el PIN de revocación del certificado y la dirección de email en la que se ha entregado, o si tienen acceso a la dirección de email en la que se ha entregado el PIN de revocación.

Camerfirma guardará los correspondientes registros de auditoría (*logs*) del servicio de revocación en línea, como evidencia de la solicitud de revocación.

Este es el procedimiento principal de solicitud de revocación para todos los tipos de certificados de entidad final, excepto para los certificados de TSU, que garantiza que Camerfirma registrará la revocación del certificado en su base de datos de certificados y publicará el estado de revocación del certificado (a través de CRL y OCSP) en un plazo inferior a 24 horas después de la recepción de la solicitud, conforme a lo dispuesto en el Reglamento eIDAS sobre la revocación de certificados cualificados.

2) Servicio de revocación a través del área privada del usuario.

   Este procedimiento está disponible para todos los tipos de certificados de entidad final, excepto los certificados de TSU y OCSP, para los que el usuario disponga de área privada configurada.

   El usuario deberá seleccionar el certificado a revocar entre los que tenga disponibles y confirmar la acción.

   Se notificará mediante correo electrónico que el proceso de revocación se ha realizado adecuadamente.

   Camerfirma guardará los correspondientes registros de auditoría (*logs*) del servicio de revocación en línea, como evidencia de la solicitud de revocación.

3) Petición enviada a un servicio web de Camerfirma.

   Este procedimiento solo estará disponible bajo proyectos específicos.

   La petición deberá contener los datos que permitan identificar el certificado o los certificados a revocar y, opcionalmente, el correspondiente motivo de revocación.

   La petición deberá estar firmada digitalmente con un certificado cualificado activo emitido por Camerfirma al solicitante de la revocación, que puede ser:

   - La Entidad (persona jurídica): el certificado utilizado debe ser un certificado emitido por Camerfirma a la Entidad, bajo una de las PC Certificado Cualificado de Sello Electrónico o Certificado Cualificado de Sello Electrónico AAPP en este documento.
   - Un tercero autorizado (persona física) para solicitar la revocación en nombre la Entidad: el certificado utilizado debe ser un certificado emitido por Camerfirma al representante legal de la Entidad, bajo una de las PC Certificado Cualificado de Representante Legal de Entidad Con/Sin Personalidad Jurídica en este documento.

Camerfirma guardará la petición firmada digitalmente recibida y los correspondientes registros de auditoría (log) del servicio web, como evidencia de la solicitud de revocación.

4) Documento de solicitud de revocación enviado a la AR a través de la cual se emitió el certificado o a la AC (Camerfirma).

   Este procedimiento está disponible para:

   - En el caso de envío del documento de solicitud a la AR, todos los tipos de certificados de entidad final, excepto los certificados de TSU y OCSP.
   - En el caso de envío del documento de solicitud a la AC, todos los tipos de certificados de entidad final, excepto los certificados OCSP de Camerfirma, y los certificados de AC Subordinadas externas.

   El documento de solicitud deberá contener los datos que permitan identificar el certificado o los certificados a revocar y, opcionalmente, el correspondiente motivo de revocación.

   El documento de solicitud deberá especificar que se solicita la revocación en horario de atención al público.

   El documento de solicitud deberá estar firmado digitalmente con un certificado válido emitido por la misma AC (el mismo certificado a revocar u otro certificado) o por otra AC de Camerfirma, con un certificado cualificado válido emitido por otro PCSC, o con un certificado válido emitido por otra AC en la que la AR o la AC confíe, o con firma manuscrita original (no escaneada), por el solicitante de la revocación,dependiendo de cada tipo de certificado, según se establece en la PC correspondiente.

   En el caso de que la firma del documento de solicitud sea manuscrita, el operador de la AR o la AC que tramita la solicitud comprobará su autenticidad, mediante cotejo con otra firma manuscrita y/o confirmación del solicitante de la revocación.

   La AR o la AC guardará el documento de solicitud recibido y registrará la fecha y hora de su recepción en horario de atención al público, como evidencia de la solicitud de revocación.

5) Personación en una oficina de la AR a través de la cual se emitió el certificado o de la AC (Camerfirma) en horario de atención al público.

   Este procedimiento está disponible, en los casos de personación en una oficina de la AR o de la AC, para todos los tipos de certificados de entidad final, excepto los certificados de TSU y OCSP.

   El solicitante de la revocación deberá identificarse ante un operador de la AR o de la AC con un documento de identidad (Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho) en vigor.

   El solicitante deberá indicar los datos que permitan identificar el certificado o los certificados a revocar y, opcionalmente, el correspondiente motivo de revocación.

   La AR o la AC guardará el documento de identidad del solicitante fotocopiado o escaneado y registrará la fecha y hora de la personación del solicitante, como evidencia de la solicitud de revocación.

6) Solicitud de revocación realizada por la AR a través de la cual se emitió el certificado o por la

AC (Camerfirma).

Este procedimiento es el único procedimiento de solicitud de revocación que está disponible también para solicitar la suspensión de un certificado y, en su caso, para solicitar su posterior reactivación.

Este procedimiento está disponible para:

- En el caso de solicitud de revocación, suspensión o reactivación realizada por la AR, todos los tipos de certificados de entidad final, excepto los certificados de TSU y OCSP.
- En el caso de solicitud de revocación realizada por la AC, todos los tipos de certificados de entidad final, incluidos los certificados de TSU y OCSP, y los certificados de AC Subordinadas bajo esta DPC y AC Subordinadas externas.
- En el caso de solicitud de suspensión o reactivación realizada por la AC, todos los tipos de certificados de entidad final, excepto los certificados de TSU y OCSP.

Para las solicitudes de revocación, suspensión o reactivación de certificados de entidad final, excepto los certificados OCSP de Camerfirma emitidos por AC Raíces y AC Subordinadas offline bajo esta DPC:

- Un operador autorizado (rol de confianza *Revocation Officers*) de la AR o de la AC solicitará la revocación, suspensión o reactivación del certificado en las plataformas de gestión de certificados. El certificado podrá ser revocado, suspendido o reactivado:
    - Individualmente, La revocación, suspensión o reactivación del certificado se realizará inmediatamente.
    - Conjuntamente con otros certificados mediante la carga de un lote con los identificadores de los certificados a revocar y la selección del motivo de revocación para todos ellos. La revocación de todos los certificados identificados en el lote se realizará a una hora programada.

  Camerfirma guardará los correspondientes registros de auditoría (logs) de las plataformas de gestión de certificados, como evidencia de la solicitud de revocación, suspensión o reactivación.
- Alternativamente, en su caso, un operador autorizado (rol de confianza *Revocation Officers*) de una AR Remota (ver sección 1.3.2), podrá solicitar la revocación del certificado en una aplicación de terceros que se comunica, mediante integración con una capa de servicios web, con las plataformas de gestión de certificados de Camerfirma (ver sección 4.1.2.4).
    - Individualmente, la revocación, suspensión o reactivación del certificado se realizará inmediatamente.

  La AR Remota guardará los correspondientes registros de auditoría (logs) de la aplicación de terceros, como evidencia de la solicitud de revocación.

  Camerfirma guardará los correspondientes registros de auditoría (logs) de las plataformas de gestión de certificados, como evidencia de la solicitud de revocación,

suspensión o reactivación.

Para las solicitudes de revocación de certificados de AC Subordinadas y de certificados OCSP de Camerfirma emitidos por AC Raíces y AC Subordinadas offline bajo esta DPC:

- Será necesaria la participación de dos operadores autorizados (rol de confianza *Revocation Officers*) de la AC para ejecutar un proceso específico en la plataforma de la AC que emitió el certificado. La revocación del certificado se realizará inmediatamente, mediante la emisión de una CRL por la AC, conteniendo el número de serie del certificado, la fecha y la hora de la revocación y el motivo de revocación especificados por los operadores.

Camerfirma registrará en un acta la emisión de la CRL, como evidencia de la solicitud de revocación.

En el caso de la revocación de certificados de TSU externas, solicitada mediante los procedimientos 4) y 6), dado el gran impacto de la revocación del certificado, Camerfirma confirmará en todo caso la solicitud de revocación con el Suscriptor del certificado.

Las AR o la AC pueden solicitar la suspensión o la revocación inmediata de un certificado mediante el procedimiento 6) de forma unilateral, por motivos de seguridad o falta de pago, sin que el Suscriptor ni el Titular puedan reclamar ninguna indemnización por este hecho.

La AR o la AC podrá, en otros casos, acordar con el Titular y/o el Suscriptor una fecha de revocación futura (ver sección 4.9.4).

Los servicios de los procedimientos 1), 2), 3) y 5) están disponibles las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de Camerfirma, Camerfirma realizará los mayores esfuerzos para asegurar que estos servicios no se encuentren inaccesibles durante más de 24 horas y, en su caso, establecerá procedimientos alternativos para solicitar la revocación de un certificado.

La notificación de hechos que pueden indicar la necesidad de revocación de certificados emitidos bajo estas DPC y PC puede ser realizada por cualquier persona interesada mediante comunicación oral o escrita con la AR a través de la cual se emitió el certificado o con la AC.

El operador de la AR o la AC deberá comprobar que la notificación procede de una fuente autorizada, que los hechos notificados son ciertos y que se corresponden con alguna de las circunstancias para la revocación contempladas en la sección 4.9.1.

El operador podrá, en su caso, solicitar documentación adicional a la persona que realiza la notificación que ayude a comprobar que los hechos notificados son ciertos (por ejemplo, un certificado de defunción del Titular/Firmante de un certificado) y/o confirmar los hechos notificados con los Titulares, Suscriptores, Entidades o terceros autorizados de los certificados afectados.

Una vez realizadas por el operador todas las comprobaciones mencionadas, la AR o la AC podrá solicitar la suspensión o revocación de los certificados afectados mediante el procedimiento 5) anteriormente indicado, después de haber informado a sus respectivos Suscriptores y Titulares.

4.9.4 PERIODO DE GRACIA DE LA SOLICITUD DE REVOCACIÓN

La AC, o cualquiera de sus AR, puede conceder un periodo de gracia de la solicitud de revocación en casos específicos que requieran una fecha de revocación futura, por ejemplo:

- Solicitud de revocación realizada mediante el procedimiento de documento de solicitud de revocación enviado a la AR a través de la cual se emitió el certificado o a la AC (Camerfirma), conforme a lo especificado en el procedimiento 3) en la sección 4.9.3.
- Revocación de un certificado de TSU, de AC Subordinada o de OCSP planificada para una fecha determinada acordada con el Suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al Titular planificada para una fecha determinada.
- Plazo de sustitución del certificado antes de su revocación acordado con el Titular y/o el Suscriptor.
- El dispositivo criptográfico donde se han generado las claves del certificado dejará de estar certificado en una determinada fecha como dispositivo cualificado de creación de firma electrónica o sello electrónico (QSCD).
- Revocación de todos los certificados activos emitidos por una AC bajo esta DPC, en caso de terminación de la AC (ver sección 5.8.2).

En estos casos, se considerará la fecha de revocación programada y la hora UTC 08:00 como el momento en que se ha producido la recepción de la solicitud y, en su caso, se permitirá, antes de dicha fecha y hora, cancelar la solicitud de revocación o posponer su fecha de revocación, por decisión del Titular y/o el Suscriptor, o por decisión de Camerfirma aceptada por el Titular y/o el Suscriptor.

4.9.5 PLAZO EN EL QUE LA AC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

Las solicitudes de revocación o suspensión y las notificaciones de hechos relacionados con la revocación serán tramitadas en el momento de su recepción.

En los casos de los procedimientos de solicitud de revocación o suspensión sin participación posterior de un operador (procedimientos 1), 2) especificados en la sección 4.9.3), la decisión de cambiar la información sobre el estado del certificado es inmediata después de la recepción de la solicitud.

En los casos de los procedimientos de solicitud de revocación con participación posterior de un operador (procedimientos 3), 4) y 5(especificados en la sección 4.9.3), el plazo máximo entre la recepción de la solicitud y la decisión de cambiar la información sobre el estado del certificado por los operadores será de 23 horas para certificados de entidad final, y de 12 horas para certificados de AC Subordinadas y de certificados OCSP de Camerfirma emitidos por AC Raíces y AC Subordinadas offline bajo esta DPC. Si la solicitud de revocación no puede confirmarse en este

plazo, entonces no es necesario cambiar el estado del certificado.

La AC procesará inmediatamente las solicitudes de revocación o suspensión después de su confirmación y registrará dichas revocaciones o suspensiones en su base de datos de certificados.

El plazo máximo entre el procesamiento de una solicitud de revocación o suspensión por la AC y el cambio real en la información sobre el estado de revocación del certificado que se pone a disposición de las Partes que Confían (a través de CRL y OCSP) es de 1 hora certificados de entidad final, excepto para los certificados OCSP de Camerfirma emitidos por AC Raíces y AC Subordinadas offline bajo esta DPC, y de 12 horas para certificados de AC Subordinadas y de certificados OCSP de Camerfirma emitidos por AC Raíces y AC Subordinadas offline bajo esta DPC.

Por tanto, cuando una AR o la AC decide revocar o suspender un certificado, la CA registrará su revocación o suspensión en su base de datos de certificados y publicará el estado de revocación del certificado (a través de CRL y OCSP) oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud, conforme a lo dispuesto en el Reglamento eIDAS sobre la revocación de certificados cualificados.

En el caso de notificaciones de hechos relacionados con la revocación, no hay un plazo máximo entre la recepción de la notificación y la decisión de cambiar la información sobre el estado del certificado, pues este plazo depende del tiempo indeterminado que el operador necesitará para comprobar que la notificación procede de una fuente autorizada, que los hechos notificados son ciertos y que se corresponden con alguna de las circunstancias para la revocación contempladas en la sección 4.9.1, conforme a lo establecido en la sección 4.9.3, si bien el operador realizará los mayores esfuerzos para que sea el menor tiempo posible.

4.9.6 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

Las Partes que Confían deben comprobar el estado de los certificados emitidos por las AC bajo esta DPC consultando la correspondiente CRL o el correspondiente servicio OCSP.

4.9.7 FRECUENCIA DE EMISIÓN DE CRL

AC	Frecuencia de emisión	Validez
CHAMBERS OF COMMERCE ROOT - 2016 **Chambers of Commerce Root - 2008**	Máximo 1 hora después de revocación / Máximo 365 días	365 días
AC CAMERFIRMA FOR NATURAL PERSONS - 2016 AC CAMERFIRMA FOR LEGAL PERSONS - 2016 AC CAMERFIRMA TSA - 2016 Camerfirma TSA II - 2014	Inmediato después de revocación / 24 horas	2 días

Camerfirma Codesign II - 2014 Camerfirma Corporate Server II - 2015 Camerfirma AAPP II – 2014		
GLOBAL CHAMBERSIGN ROOT - 2016 AC CAMERFIRMA COLOMBIA - 2016 AC CAMERFIRMA PERÚ - 2016	Máximo 1 hora después de revocación / Máximo 365 días	365 días
CAMERFIRMA ROOT 2021	Máximo 1 hora después de revocación / Máximo 365 días	365 días
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	1 hora	24 horas
INFOCERT-CAMERFIRMA CERTIFICATES 2024	Máximo 1 hora después de revocación / Máximo 365 días	365 días
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES -2024	1 hora	24 horas
INFOCERT-CAMERFIRMA TIMESTAMP 2024	Máximo 1 hora después de revocación / Máximo 365 días	365 días
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	1 hora	24 horas

En circunstancias especiales, la AC puede forzar la emisión de una CRL no planificada.

4.9.8 MÁXIMA LATENCIA PARA CRL

El tiempo máximo entre la emisión y la publicación de las CRL (máxima latencia) es:

CA	Máxima latencia
CHAMBERS OF COMMERCE ROOT – 2016 **Chambers of Commerce Root – 2008**	12 horas
AC CAMERFIRMA FOR NATURAL PERSONS – 2016	3 minutos

AC CAMERFIRMA FOR LEGAL PERSONS – 2016 AC CAMERFIRMA TSA – 2016 Camerfirma TSA II – 2014 Camerfirma Codesign II – 2014 Camerfirma Corporate Server II – 2015 Camerfirma AAPP II – 2014	
GLOBAL CHAMBERSIGN ROOT – 2016 AC CAMERFIRMA COLOMBIA – 2016 AC CAMERFIRMA PERÚ – 2016	12 horas
CAMERFIRMA ROOT 2021	12 horas
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	Inmediato
INFOCERT-CAMERFIRMA CERTIFICATES 2024	12 horas
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	Inmediato
INFOCERT-CAMERFIRMA TIMESTAMP 2024	12 horas
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	Inmediato

4.9.9 DISPONIBILIDAD DE COMPROBACIÓN EN LÍNEA DE LA REVOCACIÓN

Todas las AC bajo esta DPC proporcionan un servicio OCSP disponible 24 horas los 7 días de la semana para la comprobación en línea de la revocación de los certificados emitidos, hasta la terminación de la AC por un motivo distinto al compromiso de su clave privada (ver sección 5.8.2) o hasta el cese de actividad de Camerfirma como PSC (ver sección 5.8.1).

4.9.10 REQUISITOS DE LA COMPROBACIÓN EN LÍNEA DE LA REVOCACIÓN

Para la comprobación en línea de la revocación de un certificado emitido por una AC bajo esta DPC con el servicio OCSP de la AC:

- Camerfirma pondrá a disposición de las Partes que Confían el servicio OCSP con la posibilidad de utilizar los métodos GET y POST.
- Las respuestas del servicio OCSP estarán firmadas con el correspondiente certificado OCSP emitido por la AC o, en caso de terminación de la CA (ver sección 5.8.2), con un certificado OCSP *default* (ver sección 1.3.1.5).

- En caso de terminación de la AC por un motivo distinto al compromiso de su clave privada (ver sección 5.8.2), las respuestas del servicio OCSP para los certificados emitidos por la AC contendrán el estado *unknown*.
- Camerfirma actualizará la información proporcionada a través del servicio OCSP en el tiempo máximo indicado en la siguiente tabla tras la revocación de un certificado emitido por la AC (máxima latencia).
- Las respuestas del servicio OCSP tendrán la validez indicada en la siguiente tabla.

CA	Máxima latencia	Validez
CHAMBERS OF COMMERCE ROOT - 2016 **Chambers of Commerce Root - 2008**	12 horas	1 hora
AC CAMERFIRMA FOR NATURAL PERSONS - 2016 AC CAMERFIRMA FOR LEGAL PERSONS - 2016 AC CAMERFIRMA TSA - 2016 Camerfirma TSA II - 2014 Camerfirma Codesign II - 2014 Camerfirma Corporate Server II - 2015 Camerfirma AAPP II - 2014	10 minutos	1 hora
GLOBAL CHAMBERSIGN ROOT - 2016 AC CAMERFIRMA COLOMBIA - 2016 AC CAMERFIRMA PERÚ - 2016	12 horas	1 hora
CAMERFIRMA ROOT 2021	12 horas	1 hora
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	Inmediato	1 hora
INFOCERT-CAMERFIRMA CERTIFICATES 2024	12 horas	1 hora
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	Inmediato	1 hora
INFOCERT-CAMERFIRMA TIMESTAMP 2024	12 horas	1 hora
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	Inmediato	1 hora

4.9.11 OTRAS FORMAS DE ANUNCIOS DE REVOCACIÓN DISPONIBLES

Cuando se produce la revocación de un certificado de entidad final, se envía un comunicado mediante email al Titular especificando la fecha y hora y el motivo de la revocación.

Cuando se produce la suspensión de un certificado de entidad final, se envía un comunicado mediante email al Titular especificando la fecha y hora de la suspensión.

Si finalmente la suspensión no da lugar a la revocación definitiva y el certificado de entidad final es reactivado, cuando esto sucede, se envía un comunicado mediante email al Titular especificando la fecha y hora de la reactivación.

La fecha de la revocación de un certificado de TSU será acordada con antelación con el Suscriptor (ver sección 4.9.4).

4.9.12 REQUISITOS ESPECIALES EN RELACIÓN CON EL COMPROMISO DE CLAVES PRIVADAS

Cualquier parte que detecte el compromiso de claves privadas asociadas a certificados activos emitidos bajo esta DPC, o que sospeche de dicho compromiso, puede notificarlo a Camerfirma enviando un correo electrónico a la dirección incidentes@camerfirma.com con el asunto "Notificación de compromiso de claves", identificando los certificados asociados a las claves privadas comprometidas.

En el caso de compromiso de claves privadas asociadas a certificados de AC Raíces o Subordinadas, Camerfirma procederá conforme a lo establecido en la sección 5.7.3.

4.9.13 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

Como norma general, un certificado podrá ser suspendido debido a la sospecha no verificada completamente de alguna de las circunstancias para la revocación (ver sección 4.9.1).

El proceso de suspensión no se aplica a:

- Certificados de TSU.
- Certificados de AC Raíz y AC Subordinada.
- Certificados OCSP.
- Certificados de entidad final emitidos por las AC Subordinadas bajo esta DPC dentro de la jerarquía CAMERFIRMA ROOT 2021 (ver sección 1.3.1.3) y la jerarquía INFOCERT-CAMERFIRMA ROOT 2024 (ver sección 1.3.1.4).

4.9.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La suspensión de un certificado puede ser solicitada por:

- La AR.
- La AC (Camerfirma).

4.9.15 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

La solicitud de suspensión y, en su caso, la posterior solicitud de reactivación solo pueden ser realizadas mediante el procedimiento de solicitud de revocación 5) especificado en la sección 4.9.3.

4.9.16 LÍMITES DEL PERIODO DE SUSPENSIÓN

El periodo máximo de suspensión de un certificado es de 7 días naturales.

Camerfirma supervisa mediante un sistema de alertas de la plataforma de gestión de certificados que el periodo de suspensión no se sobrepasa.

En caso de llegar al periodo máximo de suspensión sin producirse la reactivación o la revocación definitiva el certificado, el sistema automáticamente revocará definitivamente el certificado con motivo “sin especificar”.

4.10 SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.10.1 CARACTERÍSTICAS OPERACIONALES

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

El principal servicio de consulta de estado de certificados de las AC bajo esta DPC es el proporcionado por el servicio OCSP de cada AC.

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

Cada AC Raíz bajo esta DPC, y cada AC Subordinada bajo esta DPC dentro de las jerarquías CHAMBERS OF COMMERCE ROOT 2008 y 2016 (ver sección 1.3.1.1) y GLOBAL CHAMBERSIGN ROOT 2016 (ver sección 1.3.1.2) emite una única CRL. Estas CRL mantienen los certificados revocados hasta su expiración, tras la cual se eliminan de la CRL.

El resto de Cas subordinadas definidas en esta CPS emiten una CRL para cada 50.000 certificados emitidos. Estas CRL incluyen los certificados revocados que han caducado, sin límite de tiempo después de su expiración.

Los servicios OCSP de todas las AC bajo esta DPC proporcionan información sobre el estado de los certificados que han caducado, sin límite de tiempo después de su expiración.

4.10.2 DISPONIBILIDAD DEL SERVICIO

Los servicios de comprobación del estado de los certificados están disponibles las 24 horas del día, los 7 días de la semana.

Los certificados pueden contener más de una dirección de acceso a las CRL para garantizar su disponibilidad.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de Camerfirma, Camerfirma realizará los mayores esfuerzos para asegurar que estos servicios no se encuentren inaccesibles durante más de 24 horas.

En caso de terminación de una AC bajo esta DPC (ver sección 5.8.2):

- La/s última/s CRL emitida/s por la AC conforme a lo establecido en la sección 5.8.2 estará disponible en las mismas direcciones de acceso, al menos durante 15 años después de la expiración de todos los certificados emitidos por la AC o hasta el cese de actividad de Camerfirma como PSC (ver sección 5.8.1), y, además, en el caso de las AC de Camerfirma, estarán disponibles con sus hashes SHA-1 y SHA-256 durante el mismo periodo de tiempo en el sitio web:

  https://www.camerfirma.com/autoridades-de-certificacion/

- En caso de compromiso de la clave privada de la AC (ver sección 5.7.3), el servicio OCSP seguirá proporcionando información sobre el estado correspondiente de los certificados emitidos por la AC, con respuestas firmadas con un certificado OCSP *default* (ver sección 1.3.1.5), hasta el cese de actividad de Camerfirma como PSC.

- Si no hay compromiso de la clave privada de la AC, el servicio OCSP dejará de proporcionar información sobre el estado de los certificados emitidos por la AC (las respuestas del servicio contendrán el estado *unknown* y estarán firmadas con un certificado OCSP *default*; ver sección 1.3.1.5).

En caso de cese de actividad de Camerfirma como PSC, la provisión de la información sobre el estado de revocación de los certificados emitidos por las AC de Camerfirma será garantizada por Camerfirma o por una parte confiable a quien transfiera esta obligación, a través de las últimas CRL de las AC, al menos durante 15 años después de la expiración de todos los certificados emitidos por las AC.

4.10.3 CARACTERÍSTICAS OPCIONALES

No estipulado.

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el Suscriptor y el Titular/Firmante pueden mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta DPC.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

Para certificados emitidos en QSCD Tarjeta/Token o en Tarjeta/Token, es el Titular quien custodia la clave privada en la tarjeta o token criptográfico entregado por la AR o la AC.

Para certificados emitidos en software, Camerfirma almacena las claves del Titular en formato PKCS #12 con objeto de reenviarlas en caso de problemas en su descarga e instalación. Esta información se almacena solo durante 3 días naturales. Después de este periodo, se eliminan dichas claves del sistema. Dichas claves no están incluidas en los servicios de copias de seguridad del sistema.

Para los certificados emitidos en QSCD Nube, Camerfirma almacena las claves generadas para el Titular en un HSM QSCD, proporcionando los mecanismos correspondientes para garantizar el control exclusivo de la clave privada por el Titular/Firmante o el control de la clave privada por el Titular / Creador de un Sello.

Para los certificados emitidos en Nube, Camerfirma almacena las claves generadas para el Titular en un HSM FIPS-140-2 nivel 3 o CC EAL 4 o superior, proporcionando los mecanismos correspondientes para garantizar el control exclusivo de la clave privada por el Titular/Firmante o el control de la clave privada por el Titular / Creador de un Sello.

Camerfirma no almacena la clave privada de aquellos certificados cuyas claves se hayan generado en un dispositivo externo no cualificado no gestionado por Camerfirma.

4.12.2 POLÍTICA Y PRÁCTICAS DE ENCAPSULADO Y RECUPERACIÓN DE CLAVES DE SESIÓN

No estipulado.

5 CONTROLES DE LAS INSTALACIONES, DE GESTIÓN Y OPERACIONALES

5.1 CONTROLES FÍSICOS

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

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

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

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

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año.

5.1.1 UBICACIÓN Y CONSTRUCCIÓN

Las instalaciones de Camerfirma están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta y están ubicadas en una zona de bajo riesgo de desastres naturales.

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

Para el servicio OCSP, que necesita continuidad de funcionamiento con valores de RTO/RPO cercanos a cero, algunos componentes se alojan en la nube de AWS en las regiones Europeas de Frankfurt e Irlanda.

AWS cuenta con certificaciones de conformidad según las normas ISO/IEC 27001:2022, 27017:2015, 27018:2019 e ISO/IEC 9001:2015.

5.1.2 ACCESO FÍSICO

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

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

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

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

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

El acceso a los elementos más críticos del sistema se realiza a través de tres zonas previas de paso con acceso limitado incrementalmente.

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

El acceso físico a los Centros de Datos de AWS se rige por los procedimientos de seguridad de AWS.

5.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

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

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

5.1.4 EXPOSICIÓN AL AGUA

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

5.1.5 PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

Las instalaciones técnicas de Camerfirma disponen de sistemas de detección y extinción de

incendios automáticos.

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

5.1.6 SISTEMA DE ALMACENAMIENTO

Cada medio de almacenamiento desmontable (cintas backup, CD, discos, etc.) permanece solamente al alcance de personal autorizado.

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

5.1.7 ELIMINACIÓN DE RESIDUOS

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

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para su posterior destrucción controlada.

- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para asegurar que la información contenida ha sido eliminada de forma segura.

5.1.8 COPIA DE RESPALDO EXTERNA

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

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

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

Los roles garantizan una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación, y con una concesión de mínimo privilegio, cuando sea posible.

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

- Deberes asociados a la función.
- Nivel de acceso.

- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

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

- *Security Officers* (Oficiales de Seguridad): responsabilidad general de administración de la aplicación de las prácticas de seguridad.
- *System Administrators* (Administradores de Sistemas): autorizados para instalar, configurar y mantener los sistemas de confianza del PSC para la gestión de servicios. Esto incluye la recuperación del sistema.
- *System Operators* (Operadores de Sistemas): responsables de operar los sistemas de confianza del PSC en el día a día (excluyendo las operaciones de las que son responsables los roles de confianza *Registration Officers* y *Revocation Officers*). Autorizados para realizar copias de seguridad del sistema.
- *System Auditors* (Auditores de Sistemas): autorizados para visualizar archivos y registros de auditoría (*logs*) de los sistemas de confianza del PSC.
- *Registration Officers* (Operadores de Registro): responsables de verificar la información necesaria para la emisión de certificados y aprobar las solicitudes de certificados.
- *Revocation Officers* (Operadores de Revocación): responsables de realizar los cambios de estado de los certificados.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

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

5.2.3 IDENTIFICACIÓN Y AUTENTIFICACIÓN PARA CADA ROL

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

El acceso a los recursos criptográficos se realiza mediante tarjetas criptográficas y códigos de activación.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE TAREAS

El rol de confianza *Security Officers* 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

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

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

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

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

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

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

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

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

5.3.2 PROCEDIMIENTOS DE COMPROBACIÓN DE ANTECEDENTES

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

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

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

5.3.3 REQUERIMIENTOS DE FORMACIÓN

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

La formación incluye los siguientes contenidos:

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

Camerfirma garantiza que tanto los miembros de los órganos de dirección, sus empleados, así como sus proveedores directos y sus prestadores de servicios estén informados de la importancia de la ciberseguridad, sean conscientes de las ciberamenazas asociadas a la actividad y los riesgos de su materialización. En este sentido, Camerfirma realiza acciones formativas y de sensibilizacion periódicas con el fin de incentivar la cultura de ciberseguridad y resiliencia y la aplicación de prácticas de ciber higiene conformes a las Políticas de Camerfirma y la legislación aplicable.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE LA ACTUALIZACIÓN DE LA FORMACIÓN

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

5.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No estipulado.

5.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

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

5.3.7 REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL

Los empleados contratados para realizar tareas confiables firman anteriormente las cláusulas de

confidencialidad y los requerimientos operacionales empleados por Camerfirma. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían una vez evaluados dar lugar al cese del contrato laboral.

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

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

5.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

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

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

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

5.4 PROCEDIMIENTOS DE REGISTRO DE EVENTOS

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

5.4.1 TIPOS DE EVENTOS REGISTRADOS

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

Se registrarán los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.

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

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

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

Camerfirma mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de registros de auditoría.
- Que los ficheros de registros de auditoría no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Que los ficheros de registros de auditoría se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.2 FRECUENCIA DE TRATAMIENTO DE REGISTROS DE AUDITORIA

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

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

5.4.3 PERIODOS DE RETENCIÓN PARA LOS REGISTROS DE AUDITORIA

El registro de auditoría es conservado por la AC durante 15 años (en el caso de eventos del ciclo de vida de los certificados, desde la expiración del certificado).

5.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

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

Son almacenados en dispositivos ignífugos.

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

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

Los dispositivos son manejados en todo momento por personal autorizado.

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

5.4.5 PROCEDIMIENTOS DE COPIA DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

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

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

Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA

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

ello compone el sistema de acumulación de registros de auditoría.

5.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

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

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

5.4.8 ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de Camerfirma. Anualmente se revisan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la certificación UNE-ISO/IEC 27001 que están reflejados en el documento IN-2018-11-00 – Análisis de riesgos. En este documento se especifican los controles implantados para garantizar los objetivos de seguridad requeridos.

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

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

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

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

5.5 ARCHIVO DE REGISTROS

5.5.1 TIPO DE ARCHIVOS REGISTRADOS

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

- Todos los registros de auditoría (logs) de sistema, incluyendo AC, servicios OCSP, TSU y plataformas centralizadas QSCD y No QSCD, incorporando los eventos de firma realizados.
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores,

Titulares y AR, y los datos relativos a su identificación.

- Todas las evidencias de los procesos de verificación de identidad remota por video para la emisión de certificados finales. Las evidencias comprenden: copia de la grabación del video, fotos o capturas de pantallas del solicitante y del documento de identidad utilizado, el resultado automático de la verificación realizada por el sistema, así como la evaluación y observaciones realizadas por el operador junto a su decisión de aprobación o rechazo de la identificación.
- Todas las pruebas de los procesos de identificación incompletos que no hayan llegado a término por sospecha de intento de fraude, especificándose la causa por la que no llegaron a completarse.
- Solicitudes de emisión y revocación de certificados.
- Tipo y número de documento presentado en la solicitud del certificado.
- Identidad de la AR que acepta la solicitud de certificado.
- Certificados emitidos.
- CRLs emitidas.
- DPC, PC y PDS

Camerfirma es responsable del correcto archivo de todo este material.

Camerfirma conservará estos archivos durante 15 años a contar desde la revocación o caducidad del certificado emitido, excepto los eventos en los procesos de video identificación incompletos, que los conservará durante 5 años desde la ejecución del proceso de identificación.

5.5.2 PERIODO DE RETENCIÓN PARA EL ARCHIVO

Los certificados, los contratos con los Suscriptores, la aceptación de los Términos y Condiciones, y cualquier información relativa a la identificación y autenticación del Titular y del Solicitante y, en su caso, a la identidad del Responsable serán conservados durante al menos 15 años después de la fecha de caducidad de cualquier certificado emitido en base a dicha información.

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

Las pruebas de los procesos de identificación incompletos que no hayan llegado a término por sospecha de intento de fraude se conservarán durante un plazo de 5 años desde la ejecución del proceso de identificación.

5.5.3 PROTECCIÓN DEL ARCHIVO

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

5.5.4 PROCEDIMIENTOS DE COPIA DE RESPALDO DEL ARCHIVO

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

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

5.5.5 REQUERIMIENTOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

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

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

5.5.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA

No estipulado.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

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

5.6 CAMBIO DE CLAVES

El cambio de claves de un certificado de entidad final y de un certificado OCSP es realizado mediante el proceso de una nueva emisión o, en su caso, mediante el proceso de una renovación del certificado con cambio de claves (ver apartados correspondientes en estas DPC y PC).

Las claves de las AC Raíces y las AC Subordinadas se cambiarán antes de que el certificado de la AC caduque o, en otro caso, se terminará la AC (ver sección 5.8.2).

Las claves de las AC Raíces y las AC Subordinadas también se cambiarán cuando se produce un cambio en la tecnología criptográfica (algoritmos, tamaño de claves, etc.), que lo requiera, o para cumplir con los requisitos de las normas y legislación aplicables.

Para el cambio de claves de una AC, se generará un nuevo certificado de una nueva AC, con una nueva clave privada asociada y un CN en el campo *Subject* distinto al del certificado de la AC a sustituir.

Una vez cambiadas las claves de una AC, la clave privada de la antigua AC solo se usará para firmar CRL mientras existan certificados activos emitidos por dicha AC, es decir, firmados con la clave privada de la antigua AC.

Los nuevos certificados de las AC Subordinadas de Camerfirma que emiten certificados cualificados se notificarán al Organismo de Supervisión nacional para su incorporación en la TSL.

En su caso, los nuevos certificados de las AC Raíces y las AC Subordinadas se notificarán a un repositorio de información gestionado por Mozilla, que incorpora información sobre Autoridades de Certificación – CCADB. Esta base de datos es utilizada por diversos programas comerciales para gestionar sus almacenes de confianza.

Los nuevos certificados de las AC Raíces y las AC Subordinadas bajo esta DPC se incluirán en las siguientes versiones de esta DPC y las PC. Se indicará el cambio correspondiente en la historia del documento de la versión en la que los nuevos certificados de las AC son incorporados.

Una vez cambiadas las claves de una AC, se terminará la antigua AC antes de que caduque su certificado (ver sección 5.8.2).

5.7 RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE

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

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

5.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENCIAS Y COMPROMISOS

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

El plan de continuidad y contingencias está redactado en el documento: CONF-2003-09-01 Continuidad y Disponibilidad.

Durante el tiempo que persista el incidente de compromiso de las operaciones de la AC, no se emitirán certificados.

5.7.2 CORRUPCIÓN DE RECURSOS, APLICACIONES O DATOS

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

5.7.3 COMPROMISO DE LA CLAVE PRIVADA DE LA AC

El compromiso de la clave privada de una AC, ya sea Raíz o Subordinada, se considera un evento especialmente crítico, y debe categorizarse como incidente significativo conforme a la Directiva NIS2, ya que invalida los certificados emitidos y la información sobre el estado de revocación firmados 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, Camerfirma ha establecido un procedimiento detallado a seguir dentro de su SGSI certificado en ISO 27001.

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

- Si la AC es una AC Subordinada, revocar su/s certificado/s asociado/s a la clave privada comprometida.
- Informar al Organismo de Supervisión nacional en materia de servicios de confianza, a la Autoridad de Control u organismo competente en materia de ciberseguridad y al equipo de respuesta a incidentes de seguridad de referencia (CSIRT). La notificación a estas autoridades deberá llevarse a cabo sin demora indebida y en un plazo no mayor a 24 horas, desde que se tuvo constancia de que se ha producido el incidente significativo.
- Informar a las AR afectadas, a los clientes afectados (Suscriptores y Titulares de certificados de entidad final activos emitidos por la AC, y/o Entidades propietarias de AC Subordinadas externas con certificados activos emitidos por la AC), a las Partes que Confían y a otras entidades afectadas con las que tenga acuerdos u otro tipo de relaciones, a través de comunicación directa cuando sea posible, y a través de comunicación en el sitio web de Camerfirma.
- Indicar en las informaciones anteriores:
    - En caso de su conocimiento, fecha y hora en que se produjo o se sospecha que se produjo el compromiso de la clave privada de la AC.
    - Que los certificados y la información sobre el estado de revocación firmados con la clave privada comprometida de la AC pueden ya no ser válidos.
    - Medidas tomadas y/o planeadas para invalidar la clave privada comprometida de la AC (revocación de su/s certificado/s asociados) y para proporcionar de forma fiable la información sobre el estado de revocación de los certificados emitidos por la AC.
- Terminar la AC (ver sección 5.8.2).

Una vez terminada la AC conforme a lo establecido en la sección 5.8.2, Camerfirma seguirá

proporcionando de forma fiable información sobre el estado de revocación de los certificados emitidos por la AC, a través de la/s última/s CRL y el servicio OCSP en las mismas direcciones de acceso, sin usar la clave privada comprometida ni un certificado OCSP firmado con la clave privada comprometida, de la forma siguiente:

- La/s última/s CRL será/n firmada/s con una nueva clave privada asociada a un nuevo certificado de la AC con el mismo campo *subject.*

  En caso de compromiso de la clave privada de una AC Subordinada, el nuevo certificado de la AC será emitido por la misma AC emisora o por otra AC de Camerfirma bajo la misma jerarquía.

  En caso de compromiso de la clave privada de una AC Raíz, el nuevo certificado de la AC será emitido por otra AC de Camerfirma bajo otra jerarquía de Camerfirma.

- El servicio OCSP seguirá proporcionando información sobre el estado de los certificados emitidos por la AC, pero las respuestas del servicio estarán firmadas con un certificado OCSP *default* emitido por otra CA (ver sección 1.3.1.5).

Camerfirma podrá sustituir la AC con la clave comprometida por una nueva AC o por otra AC existente, y ofrecer nuevos certificados emitidos por esta CA a los clientes afectados.

5.7.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

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

5.8 TERMINACIÓN DE UNA AC O UNA AR

5.8.1 CESE DE ACTIVIDAD

Antes de que Camerfirma cese su actividad como PSC emisor de certificados cualificados:

- 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.
- Comunicará al Organismo de Supervisión nacional, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra Camerfirma, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad de Camerfirma como PSC emisor de certificados cualificados.
- Notificará al Organismo de Supervisión nacional el cese de su actividad como PSC emisor de certificados cualificados y, en su caso, la parte confiable a la que transferirá cualquier obligación (véase más adelante), con al menos dos meses de antelación.
- Notificará el cese de la actividad a los clientes afectados (Suscriptores y Titulares de certificados activos afectados) y a otras entidades afectadas con las que tenga acuerdos u

otro tipo de relaciones, con al menos dos meses de antelación.

- Publicará la información pertinente relativa al cese de la actividad en su página web y/o en cualquier otro medio accesible a las Partes que Confían, con al menos dos meses de antelación.
- Revocará cualquier autorización a entidades subcontratadas para actuar en nombre de Camerfirma en cualquier función relacionada con el proceso de emisión de certificados cualificados.
- Terminará cualquier AC de Camerfirma afectada (ver sección 5.8.2).
- Seguirá cumpliendo, con respecto a las AC afectadas, sus obligaciones de conservar la información de registro y los archivos de registro de eventos, y de proporcionar los certificados de las AC y la información sobre el estado de revocación de los certificados emitidos, durante el período de tiempo indicado a los Suscriptores, Titulares, Responsables y Partes que Confían (15 años después de la expiración de los certificados), o transferirá estas obligaciones a una parte confiable.

Todas estas actividades se incluyen de forma detallada en el Plan de Cese de Servicios de Confianza Cualificados de Camerfirma.

Antes de que Camerfirma cese su actividad como PSC emisor de certificados no cualificados:

- 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.
- Notificará el cese de la actividad a los clientes afectados (Suscriptores y Titulares de certificados de entidad final activos afectados, y/o Entidades propietarias de AC Subordinadas externas con certificados activos afectados) y otras entidades afectadas con las que tenga acuerdos u otro tipo de relaciones.
- Publicará la información pertinente relativa al cese de la actividad en su página web y/o en cualquier otro medio accesible a las Partes que Confían.
- Revocará cualquier autorización a entidades subcontratadas para actuar en nombre de Camerfirma en cualquier función relacionada con el proceso de emisión de certificados no cualificados.
- Terminará cualquier AC de Camerfirma afectada (ver sección 5.8.2).
- Seguirá cumpliendo, con respecto a las AC afectadas, sus obligaciones de conservar la información de registro y los archivos de registro de eventos, y de proporcionar los certificados de las AC y la información sobre el estado de revocación de los certificados emitidos, durante el período de tiempo indicado a los Suscriptores, Titulares, Responsables y Partes que Confían (15 años después de la expiración de los certificados), o transferirá estas obligaciones a una parte confiable.

De acuerdo con la Ley 6/2020, Camerfirma notificará el cese de su actividad como PSC emisor de certificados no cualificados al Organismo de Supervisión nacional y, en su caso, la parte confiable a la que ha transferido cualquier obligación, en el plazo de tres meses después de dicho cese.

5.8.2 TERMINACIÓN DE UNA AC

Camerfirma terminará cualquier AC bajo esta DPC en caso de compromiso de su clave privada o por otros motivos, como, por ejemplo, la expiración de su certificado o el cese de la actividad de Camerfirma como PSC emisor de certificados cualificados y/o como PSC de certificados no cualificados (ver sección 5.8.1).

Antes de que Camerfirma termine una AC bajo esta DPC por compromiso de su clave privada, conforme a lo establecido en la sección 5.7.3:

- Si la AC es una AC Subordinada, revocará su/s certificado/s asociado/s a la clave privada comprometida.
- Informará al Organismo de Supervisión nacional, a las AR afectadas, a los clientes afectados, a las Partes que Confían y a otras entidades afectadas con las que tenga acuerdos u otro tipo de relaciones.

Antes de que Camerfirma termine una AC bajo esta DPC por un motivo distinto al compromiso de su clave privada:

- Si la AC tiene certificados emitidos de entidad final activos, notificará la terminación de la AC a sus respectivos Suscriptores y Titulares y, en el caso de que la AC sea sustituida por una nueva AC o por otra AC existente, les ofrecerá nuevos certificados emitidos por esta AC.
- Si la AC tiene certificados emitidos de AC Subordinadas externas activos, notificará la terminación de la AC a sus respectivas Entidades propietarias, y, en el caso de que la AC sea sustituida por una nueva AC o por otra AC existente, les ofrecerá nuevos certificados emitidos por esta AC.
- En su caso, notificará la terminación de la AC a otras entidades afectadas con las que tenga acuerdos u otro tipo de relaciones.

Camerfirma terminará una AC bajo esta DPC cuando haya finalizado las siguientes acciones:

- Dejará de emitir certificados por la AC.
- Revocará todos los certificados activos emitidos por la AC.
- En el caso de que la AC figure en la Lista de Confianza (TSL) nacional como un servicio de expedición de certificados cualificados con estado actual *granted*, solicitará al Organismo de Supervisión nacional su cambio de estado a *withdrawn*.
- Después de la revocación de todos los certificados activos emitidos por la AC, emitirá y publicará la/s última/s CRL de la AC, que incluirá/n los certificados revocados que han caducado y tendrá/n una validez hasta el 31/12/9999 hora UTC.

  En caso de compromiso de la clave privada de la AC, la/s última/s CRL será/n firmada/s con una nueva clave privada asociada a un nuevo certificado de la AC, conforme a lo establecido en la sección 5.7.3.

- Si no hay compromiso de la clave privada de la AC, el servicio OCSP de la AC dejará de proporcionar información sobre el estado de los certificados emitidos por la AC (las respuestas del servicio contendrán el estado *unknown* y estarán firmadas con un certificado OCSP *default*; ver sección 1.3.1.5).

  En caso de compromiso de la clave privada de la AC, el servicio OCSP seguirá proporcionando información sobre el estado correspondiente de los certificados emitidos por la AC, con respuestas firmadas con un certificado OCSP *default* (ver sección 1.3.1.5).

- Después de la emisión de la/s última CRL, si la AC es una AC Subordinada, su/s certificado/s será/n revocado/s por la correspondiente AC emisora o expirará/n.

  En caso de compromiso de la clave privada de la AC, será revocado su nuevo certificado asociado a la nueva clave privada usada para firmar la/s últimas CRL (su/s certificado/s asociado/s a la clave privada comprometida de la AC ya habrán sido revocados con anterioridad, conforme a lo establecido en la sección 5.7.3).

- Después de la emisión de la/s última/s CRL, destruirá la clave privada de la AC, incluyendo todas las copias de seguridad identificadas por Camerfirma, de una forma que impida su recuperación, y conforme a un procedimiento establecido previamente.

  En caso de compromiso de la clave privada de la AC, también destruirá la nueva clave privada de la AC asociada al nuevo certificado de la AC, de la misma forma.

- En su caso, notificará al Organismo de Supervisión nacional y/o a otras entidades afectadas con las que tenga acuerdos u otro tipo de relaciones la terminación efectiva de la AC y/o las acciones realizadas.

Camerfirma dará por terminada cualquier AC Subordinada externa dentro de las jerarquías bajo esta DPC cuando su/s certificado/s sea/n revocado/s por la correspondiente AC emisora.

Una vez terminada una AC, no se incluirá en las siguientes versiones de estas DPC y PC. Se indicará el cambio correspondiente en la historia del documento de la versión en la que la AC es eliminada.

Camerfirma dará por terminada una de las PC en este documento cuando no haya certificados activos emitidos bajo esa PC por la/s correspondiente/s AC emisora/s.

Una vez terminada una PC, no se incluirá en las siguientes versiones de estas DPC y PC. Se indicará el cambio correspondiente en la historia del documento de la versión en la que la PC es eliminada.

5.8.3 TERMINACIÓN DE UNA AR

En caso de terminación de una AR:

- La AC dejará de emitir certificados a través de la AR.
- La AC revocará todos los certificados activos emitidos a través de esa AR, excepto que exista un acuerdo entre la AC y la AR para mantenerlos activos.
- La AR entregará a la AC la información y documentación que ha sido necesaria para la emisión y gestión de los certificados a través de la AR.

- La AR proporcionará a la AC toda la información existente acerca de las solicitudes de certificados en curso y todavía no validadas, para que la AC pueda validarlas una vez comprobado el cumplimiento de los requisitos de las correspondientes PC aplicables.
- La AR garantizará que mantendrá, de forma indefinida, la confidencialidad a la que ha estado obligada en virtud del contrato con la AC.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

Los equipos usados por Camerfirma para albergar claves raíces están certificados FIPS 140-2 nivel 3 o CC EAL 4 o superior.

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

La creación de claves de AC Subordinadas se genera en equipos HSM certificados FIPS 140-2 nivel 3 o CC EAL 4 o superior donde se albergarán para su correspondiente uso.

AC	Longitud de claves	Algoritmo de firma	Creación	Caducidad
CHAMBERS OF COMMERCE ROOT – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	08/04/2040
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
AC CAMERFIRMA FOR LEGAL PERSONS - 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
AC CAMERFIRMA TSA – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
Chambers of Commerce Root – 2008 (certificado SHA-1)	4096 bits	sha1WithRSAEncryption	01/08/2008	31/07/2038
Chambers of Commerce Root – 2008 (certificado SHA-256)	4096 bits	sha256WithRSAEncryption	07/12/2011	31/07/2038
Camerfirma TSA II – 2014	4096 bits	sha256WithRSAEncryption	16/12/2014	15/12/2037
Camerfirma Codesign II – 2014	4096 bits	sha256WithRSAEncryption	16/12/2014	15/12/2037
Camerfirma Corporate Server II - 2015	4096 bits	sha256WithRSAEncryption	15/01/2015	15/12/2037
Camerfirma AAPP II – 2014	4096 bits	sha256WithRSAEncryption	16/12/2014	15/12/2037
GLOBAL CHAMBERSIGN ROOT – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	08/04/2040

AC CAMERFIRMA COLOMBIA – 2016	4096 bits	sha256WithRSAEncryption	14/04/2016	09/03/2040
AC CAMERFIRMA PERÚ – 2016	4096 bits	sha256WithRSAEncryption	11/10/2016	10/03/2040
CAMERFIRMA ROOT 2021	4096 bits	sha384WithRSAEncryption	19/10/2021	13/10/2045
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	4096 bits	sha384WithRSAEncryption	20/10/2021	16/10/2037
INFOCERT-CAMERFIRMA CERTIFICATES 2024	384 bits	sha384ECDSA	22/01/2024	22/01/2045
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	384 bits	sha384ECDSA	16/02/2024	16/02/2040
INFOCERT-CAMERFIRMA TIMESTAMP 2024	384 bits	sha384ECDSA	22/01/2024	22/01/2045
INFOCERT- CAMERFIRMA QUALIFIED TSA - 2024	384 bits	Sha384ECDSA	16/02/2024	16/02/2040

6.1.1.1 GENERACIÓN DEL PAR DE CLAVES DEL TITULAR

Las claves del Titular pueden ser creadas por él mismo mediante dispositivos Tarjeta/Token o software autorizados por Camerfirma, o pueden ser creadas por las AR en dispositivos Tarjeta/Token autorizados por Camerfirma, o pueden ser creadas por Camerfirma en formato software PKCS #12.

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

- Las plataformas de gestión de certificados de Camerfirma generan con sus propios recursos una contraseña aleatoria robusta y una clave privada protegida con dicha contraseña usando el algoritmo AES. A partir de esa clave privada genera una petición de firma de certificado en formato PKCS #10. Con esa petición la AC realiza la firma del certificado del Titular. El certificado es entregado al Responsable en un fichero PKCS #12 en el que se incluye el propio certificado y la clave privada asociada a él. La contraseña de la clave privada y del fichero PKCS #12 nunca está en claro en el sistema.

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

- Las claves también pueden ser creadas en un sistema remoto usando la capa de servicios WEB para generar una solicitud PKCS #10 y la recogida del certificado correspondiente.
- En un sistema de gestión centralizada de claves, cualificado o no cualificado, las claves son

generadas y almacenadas en un dispositivo de creación de firma que se ajusta, por lo menos, a los requisitos que se establecen en el Anexo II del Reglamento eIDAS.

Las claves tienen una longitud mínima de 2048 bits (RSA) o 256 bits (ECDSA).

6.1.1.2 HARDWARE/SOFTWARE DE GENERACIÓN DE CLAVES

Las claves de los Titulares pueden ser generadas por ellos mismos en un dispositivo autorizado por Camerfirma. Ver apartado 6.1.1.1

Las claves de las AC utilizan un dispositivo criptográfico que cumple las especificaciones FIPS 140-2 nivel 3 o CC EAL 4 o superior.

6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ver apartado 3.2.1.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

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

6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LOS USUARIOS

Ver sección 2.2.3.

6.1.5 TAMAÑO DE LAS CLAVES

Las claves de los certificados de AC para las AC Raíces y Subordinadas activas dentro de las jerarquías bajo esta DPC están basadas en el algoritmo RSA o ECDSA, con una longitud de 4096 bits (RSA) o 384 bits (ECDSA). Ver apartado 6.1.1.

Las claves de los certificados de entidad final están basadas en el algoritmo RSA o ECDSA con una longitud mínima de 2048 bits (RSA) o 256 bits (ECDSA).

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

La clave pública de los certificados de AC para las AC Raíces y Subordinadas activas dentro de las jerarquías bajo esta DPC y la clave pública de los certificados de entidad final bajo estas DPC y PC están codificadas de acuerdo con los estándares IETF RFC 5280 y PKCS #1. El algoritmo de generación de claves es RSA o ECDSA.

- Algoritmo de generación de claves: rsagen1 / ECDSA.
- Método de relleno: emsa-pkcs1-v1_5 / ECDSA.
- Funciones criptográficas de hash: SHA-1 (solo en certificados de AC para AC Raíces emitidos en 2008), SHA-256, SHA-384, SHA-512.

6.1.7 PROPÓSITOS DE USO DE CLAVES

Todos los certificados emitidos contienen las extensiones *Key Usage* y *Extended Key Usage*, como se definen en el estándar IETF RFC 5280. Más información disponible en las secciones 4.5.1 y 7.1.2.

Las claves privadas de las AC Raíces no deben utilizarse para firmar certificados de entidad final, sino únicamente para firmar los siguientes certificados:

- Certificados autofirmados de la AC Raíz.
- Certificados de AC Subordinadas bajo esta DPC y AC Subordinadas externas.
- Certificados OCSP.

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

6.2.1 CONTROLES Y ESTÁNDARES DE MÓDULOS CRIPTOGRÁFICOS

6.2.1.1 CLAVE PRIVADA DE LA AC

La clave privada de firma de las AC Raíz y las AC Subordinadas es generada y almacenada en HSM que cumplen las especificaciones FIPS 140-2 nivel 3 o CC EAL 4 o superior y que son manejados por al menos dos operadores en un modelo n de m. Los HSM están albergados en entornos seguros.

Los HSM que almacenan las claves de las AC Raíz se gestionan dentro de una sala criptográfica aislada y desconectada. Los HSM que almacenan las claves de las AC Subordinadas se alojan en entornos seguros dentro de un CPD siguiendo normativa ISO27001.

Cuando la clave privada de la AC está fuera del HSM, se mantiene cifrada.

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

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

6.2.1.2 CLAVE PRIVADA DEL TITULAR

La clave privada del Titular se puede generar y almacenar en un dispositivo software (PKCS #12), tarjeta/token, plataforma centralizada, HSM (certificado de TSU o AC) o dispositivo externo (PKCS #10).

En software (PKCS #12), Camerfirma ofrece instrucciones de configuración para un uso seguro.

En QSCD Tarjeta/Token, las claves son generadas y almacenadas en un dispositivo tarjeta/token criptográfico QSCD, que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS, y por tanto son aptas para la creación de firmas electrónicas cualificadas y sellos electrónicos cualificados.

En Tarjeta/Token (tarjeta/token No QSCD o QSCD), las claves son generadas y almacenadas en un dispositivo tarjeta/token criptográfico FIPS 140-2 nivel 3 o CC EAL 4 o superior, No QSCD o QSCD.

En QSCD Nube (plataforma centralizada QSCD), las claves son generadas y almacenadas en un HSM QSCD, de una forma que permite al Titular/Firmante (o al Titular/ Creador de un Sello, en el caso de persona jurídica) acceder a la clave privada bajo su control exclusivo (o bajo su control, en el caso de persona jurídica), y que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS, y por tanto son aptas para la creación de firmas electrónicas cualificadas y sellos electrónicos cualificados.

En Nube (plataforma centralizada No QSCD o QSCD), las claves son generadas y almacenadas en un HSM FIPS 140-2 nivel 3 o CC EAL 4 o superior, No QSCD o QSCD, de una forma que permite al Titular/Firmante (o al Titular/ Creador de un Sello, en el caso de persona jurídica) acceder a la clave privada bajo su control exclusivo (o bajo su control, en el caso de persona jurídica).

En QSCD HSM (certificado de TSU), las claves son generadas y almacenadas en un HSM QSCD, que se ajusta a los requisitos que se establecen en el Anexo II del Reglamento eIDAS, y por tanto son aptas para la creación de sellos electrónicos cualificados.

En HSM (certificado de TSU o AC) No QSCD o QSCD, las claves son generadas y almacenadas en un HSM FIPS 140-2 nivel 3 o FIPS 140-3 nivel 3 o CC EAL 4 o superior, No QSCD o QSCD.

En dispositivo externo (PKCS #10), No QSCD o QSCD, las claves son generadas y almacenadas en un dispositivo externo no gestionado por Camerfirma, por lo que Camerfirma no puede garantizar que dicho dispositivo sea QSCD y por este motivo se cataloga como No QSCD.

Camerfirma comprobará la conformidad de los dispositivos QSCD Tarjeta/Token, QSCD Nube y QSCD HSM utilizados con el Reglamento eIDAS, bien con la última lista de QSCD publicada por la Comisión Europea, o bien mediante notificación del Organismo de Supervisión, o bien mediante notificación del PCSC que gestiona el dispositivo QSCD Nube, o bien mediante notificación del PSC que gestiona el dispositivo QSCD HSM. Si Camerfirma detecta en estas comprobaciones que alguno de estos dispositivos deja de tener la consideración de QSCD, Camerfirma revocará todos los certificados activos en los que la clave privada se encuentre en dichos dispositivos.

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

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

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

6.2.3 DEPÓSITO DE CLAVE PRIVADA

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

Excepciones:

- En caso de certificados para cifrado de información Camerfirma guarda una copia de dicha clave.
- En una plataforma centralizada, QSCD o no QSCD, las claves son generadas y almacenadas en un dispositivo de creación de firma que se ajusta, por lo menos, a los requisitos que se establecen en el Anexo II del Reglamento eIDAS.

6.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

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

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

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

Las claves del Titular en Tarjeta/Token no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

En una plataforma centralizada, QSCD o no QSCD, se pueden realizar copias de seguridad de las claves del Titular en los términos marcados por la reglamentación correspondiente.

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

6.2.5 ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas de las AC no son archivadas después de la terminación de la CA porque son destruidas (ver sección 5.8.2)

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

Solo en caso de certificados de cifrado el Titular podrá almacenar la clave privada el tiempo que

crea oportuno. En este caso Camerfirma también guardará copia de la clave privada asociada al certificado de cifrado.

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

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

6.2.6 INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Las claves de las AC se crean en el interior de los dispositivos criptográficos.

Las claves en software de los Titulares se crean en los sistemas de Camerfirma y son entregadas al Titular en un dispositivo software PKCS #12.

Las claves en Tarjeta/Token de los Titulares se crean dentro del dispositivo criptográfico entregado por la AC.

En una plataforma centralizada, QSCD o no QSCD, según la descripción en el manual del fabricante del dispositivo.

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

Las claves asociadas a los Titulares no pueden ser trasferidas.

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

6.2.7 ALMACENAMIENTO DE CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

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

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

En una plataforma centralizada, QSCD o no QSCD, según la descripción en el manual del fabricante del dispositivo.

6.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

El acceso a la clave privada del Titular se realiza por medio de una clave de activación que conocerá solamente el Titular y que Camerfirma recomienda no tener por escrito.

La clave de la AC Raíz se activa por un proceso de n de m. Ver apartado 6.4.

La activación de las claves privadas de la AC Subordinadas son gestionadas por el aplicativo de gestión.

En una plataforma centralizada, QSCD o no QSCD, según consta en la descripción en el manual del

fabricante del dispositivo entregado al titular después de la validación de su identidad o solicitándolo en https://www.camerfirma.com/contacto-soporte/

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

6.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Para los certificados en Tarjeta/Token, la clave privada del Titular quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

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

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

Para claves de entidad AC Raíz, AC Subordinada y TSU, se realizará una ceremonia criptográfica de la que se elaborará el acta correspondiente.

En una plataforma centralizada, QSCD o no QSCD, según consta en la descripción en el manual del fabricante del dispositivo entregado al titular después de la validación de su identidad o solicitándolo en https://www.camerfirma.com/contacto-soporte/

6.2.10 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

Con anterioridad a la destrucción de las claves privadas se revocarán los certificados asociados a la mismas.

Se realizará un borrado seguro de la clave privada de la AC en los dispositivos criptográfico (HSM) que la tengan almacenada, siguiendo los pasos descritos en el manual de administración del HSM. Finalmente, se realizará un borrado seguro de todas las copias de seguridad de la clave privada.

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

Las claves del Titular en Tarjeta/Token podrán ser destruidas mediante un software especial en los puntos de Registro o en la AC.

En una plataforma centralizada, QSCD o no QSCD, según consta en la descripción en el manual del fabricante del dispositivo entregado al titular después de la validación de su identidad o solicitándolo en https://www.camerfirma.com/contacto-soporte/

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

6.2.11 CALIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

Según lo estipulado en el apartado 6.2.1.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

La AC mantendrá sus archivos durante un periodo mínimo de quince años siempre y cuando la tecnología de cada momento lo permita. Dentro de la documentación a custodiar se encuentran los certificados de clave pública emitidos a sus Titulares y los certificados de clave pública propios.

6.3.2 PERIODO DE USO PARA LAS CLAVES PÚBLICAS Y PRIVADAS

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

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

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

Todos los certificados emitidos por Camerfirma son válidos desde el momento de su firma hasta el momento de su caducidad.

Los periodos de validez de los certificados bajo estas DPC y PC son:

- Certificados de las AC Raíz y Subordinadas activas dentro de las jerarquías bajo esta DPC: ver sección 6.1.1.
- Certificados OCSP (ver sección 1.3.1.5): 1 año.
- Certificados cualificados emitidos por las AC Subordinadas de Camerfirma: máximo 5 años.
- Certificados no cualificados emitidos por las AC Subordinadas de Camerfirma: máximo 6 años.

6.4 DATOS DE ACTIVACIÓN DE LAS CLAVES PRIVADAS

6.4.1 GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la clave privada del Titular se generan de diferente forma según el tipo de certificado.

En software. El certificado se genera por la CA y se entrega en un fichero estandarizado PKCS #12 protegido por una contraseña que será entregada al Responsable mediante el correo electrónico asociado al certificado.

En Dispositivo Tarjeta/Token. Las tarjetas utilizadas por Camerfirma se generan en el puesto de

registro protegidas con un PIN y PUK calculado de fábrica. Esta información es enviada por la plataforma de gestión al Titular mediante el correo electrónico asociado al certificado. El Titular dispone de un software para cambiar el PIN y PUK de su tarjeta.

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

En una plataforma centralizada, QSCD o no QSCD, las claves se generan en un dispositivo criptográfico HSM protegido por una clave maestra del dispositivo y por los datos de activación de la clave generada y conocida solo por el propio Responsable del certificado asociado. La plataforma permite activar un doble control de activación vía OTP.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación son comunicados al Titular por un canal independiente a la plataforma de gestión PKI. Camerfirma no almacena dicha información custodiada en su base de datos para los certificados en formato software o Tarjeta/Token. Camerfirma no los almacena para certificados en la plataforma centralizada, pues son conocidos y custodiados por el Titular. Los datos pueden ser enviados de nuevo al Titular bajo solicitud previa al correo electrónico asociado al certificado, y serán eficaces siempre que el Titular no haya realizado un cambio en ellos previamente.

En una plataforma centralizada, QSCD o No QSCD, según consta en la descripción en el manual del fabricante del dispositivo entregado al titular después de la validación de su identidad.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulado.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

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

Respecto a la seguridad de la información se sigue el esquema de certificación sobre sistemas de gestión de la información ISO 27001.

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

1) Configuración de seguridad del sistema operativo.
2) Configuración de seguridad de las aplicaciones.
3) Dimensionamiento correcto del sistema.

4) Configuración de Usuarios y permisos.
5) Configuración de eventos de registros de auditoría.
6) Plan de copia de respaldo y recuperación.
7) Configuración antivirus.
8) Requerimientos de trafico de red.

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD INFORMÁTICA ESPECÍFICOS

Cada servidor de Camerfirma incluye las siguientes funcionalidades:

- control de acceso a los servicios de AC y gestión de privilegios.
- imposición de separación de tareas para la gestión de privilegios.
- identificación y autenticación de roles asociados a identidades.
- archivo del historial del Titular y la AC y datos de auditoría.
- auditoria de eventos relativos a la seguridad.
- autodiagnóstico de seguridad relacionado con los servicios de la AC.
- mecanismos de recuperación de claves y del sistema de AC.

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

6.5.2 VALORACIÓN DE LA SEGURIDAD INFORMÁTICA

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

Camerfirma mantiene un proceso continuado de gestión del riesgo para garantizar la seguridad de las redes y de la información y la ciber resiliencia de sus operaciones. A estos fines, revisa y, en su caso, actualiza los resultados de la evaluación de riesgos y el plan de tratamiento de riesgos a intervalos planificados al menos una vez al año, o cuando se produzcan cambios significativos en las operaciones, en los riesgos o tras la gestión de incidentes significativos.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Respecto a los dispositivos tarjeta/token:

1) Los dispositivos QSCD Tarjeta/Token están certificados QSCD. Los dispositivos tarjeta/token No QSCD o QSCD están certificados FIPS 140-2 nivel 3 o CC EAL 4 o superior.
2) Los dispositivos son preparados y estampados por un proveedor externo.
3) La gestión de distribución del soporte la realiza el proveedor externo que lo distribuye a las AR para su entrega al Titular.

4) El Titular o la AR utiliza el dispositivo para generar el par de claves y enviar la clave pública a la AC.
5) La AC envía un certificado de clave pública al Titular o la AR que es introducido en el dispositivo.
6) El dispositivo es reutilizable y puede mantener de forma segura varios pares de claves.
7) El dispositivo queda en propiedad del Titular.

Respecto a los dispositivos plataforma centralizada:

- Los dispositivos QSCD Nube utilizan un HSM para almacenar las claves certificado QSCD, y están autorizados por el Organismo de Supervisión para los servicios catalogados como *QSCDManagedOnBehalf*.
- Los dispositivos plataforma centralizada No QSCD o QSCD utilizan un HSM para almacenar las claves certificado FIPS 140-2 nivel 3 o CC EAL 4 o superior.

6.6.1 CONTROLES DE DESARROLLO DEL SISTEMA

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

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

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

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

6.6.2 CONTROLES DE GESTIÓN DE LA SEGURIDAD

6.6.2.1 GESTIÓN DE SEGURIDAD

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

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

Camerfirma exige mediante contrato, las medidas de seguridad equivalentes a cualquier

proveedor externo implicado en las labores de certificación.

6.6.2.2 CLASIFICACIÓN Y GESTIÓN DE INFORMACIÓN Y BIENES

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

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

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

6.6.2.3 OPERACIONES DE GESTIÓN

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

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

6.6.2.4 TRATAMIENTO DE LOS SOPORTES Y SEGURIDAD

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

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

6.6.2.5 PLANIFICACIÓN DEL SISTEMA

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

6.6.2.6 REPORTES DE INCIDENCIAS Y RESPUESTA

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

incidencia.

6.6.2.7 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

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

6.6.2.8 GESTIÓN DEL SISTEMA DE ACCESO

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

General:

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

Generación del certificado:

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

Gestión de la revocación:

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

Estado de la revocación:

La aplicación del estado de la revocación (OCSP) dispone de un control de acceso mediante autenticación fuerte para evitar el intento de modificación de la información del estado de la revocación.

6.6.3 GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

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

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

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

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

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

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

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

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

6.6.4 EVALUACIÓN DE LA SEGURIDAD DEL CICLO DE VIDA

No estipulado.

6.7 CONTROLES DE SEGURIDAD DE LA RED

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

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

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

Los sistemas de administración y los sistemas de producción están en entornos separados.

6.8 FUENTES DE TIEMPO

Camerfirma dispone de un procedimiento de sincronización de tiempo coordinado con el ROA (Real Instituto y Observatorio de la Armada) en San Fernando vía NTP. También obtiene una

fuente segura vía GPS y sincronización vía Radio.

7 PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 PERFILES DE CERTIFICADOS

Los perfiles de los certificados bajo estas DPC y PC cumplen los estándares IETF RFC 5280 e ITU-T X.509 y los estándares ETSI EN 319 412 aplicables.

Los perfiles de los certificados cualificados bajo estas DPC y PC cumplen el estándar IETF RFC 3739 y los estándares ETSI EN 319 412 aplicables.

Camerfirma publica las fichas de los perfiles de certificados bajo esta DPC y las PC en el sitio web https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/.

7.1.1 NÚMERO DE VERSIÓN

Todos los certificados son X.509 versión 3.

7.1.2 EXTENSIONES DEL CERTIFICADO

Las extensiones de los certificados se encuentran detalladas en las fichas de los perfiles de certificados (ver sección 7.1).

7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

El OID del algoritmo de firma puede ser:

- 1.2.840.113549.1.1.5 - sha1WithRSAEncryption (solo en certificados de AC para AC Raíces emitidos en 2008)
- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption
- 1.2.840.113549.1.1.12 - sha384WithRSAEncryption
- 1.2.840.113549.1.1.13 - sha512WithRSAEncryption
- 1.2.840.10045.4.3.2 – sha256WithECDSAEncryption
- 1.2.840.10045.4.3.3 – sha384WithECDSAEncryption

El OID del algoritmo de clave pública en el campo *Subject Public Key Info* puede ser:

- 1.2.840.113549.1.1.1 – *rsaEncryption*
- *1.2.840.10045.2.1 - ECC*

Los OID de los algoritmos se encuentran especificados en las fichas de los perfiles de certificados (ver sección 7.1).

7.1.4 FORMATO DE LOS NOMBRES

Los certificados contienen los datos del Titular (nombres) que resulten necesarios para su uso en el campo *Subject* y, en su caso, en la extensión *Subject Alternative Name*, de acuerdo con lo establecido en esta DPC y las PC.

En general, los certificados para uso en el sector público deben incluir los siguientes datos del Titular en el campo *Subject* y, en su caso, en la extensión *Subject Alternative Name*:

- En su caso, nombre y apellidos de la persona física Titular en campos separados.
- En su caso, denominación social de la Entidad (persona jurídica o entidad sin personalidad jurídica).
- Números de documentos de identidad de la persona física Titular y/o la Entidad, de acuerdo con la legislación aplicable.

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

El formato y la semántica de los datos incluidos en el campo *Subject* y, en su caso, en la extensión *Subject Alternative Name* se describen en las fichas de los perfiles de certificados (ver sección 7.1).

7.1.5 RESTRICCIONES DE LOS NOMBRES

Camerfirma puede definir restricciones de los nombres (ver sección 7.1.4) en los certificados de AC Subordinadas externas, mediante la extensión *Name Constrains,* de forma que estas AC solo puedan emitir certificados con nombres que cumplan las restricciones definidas en dicha extensión.

7.1.6 IDENTIFICADOR DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICACIÓN

Los certificados de entidad final contienen un OID de PC, que parte de la base 1.3.6.1.4.1.17326, que identifica la PC de Camerfirma aplicable.

Los certificados de entidad final pueden contener los OID de PC aplicables definidos en la normativa nacional, y/o en estándares ETSI, y/o en otra normativa aplicable.

Los certificados de AC, en general, contienen el OID de PC 2.5.29.32.0 (*anyPolicy*), pero, en algunos casos, pueden contener otro/s OID.

Los OID de PC contenidos en los certificados se encuentran especificados en las fichas de los perfiles de certificados (ver sección 7.1), y en las PC de cada tipo de certificado.

7.1.7 USO DE LA EXTENSIÓN "POLICY CONSTRAINTS"

Camerfirma puede definir restricciones de las políticas en los certificados de AC Subordinadas externas, mediante la extensión *Policy Constraints*, de forma que estas AC solo puedan emitir

certificados con políticas que cumplan las restricciones definidas en dicha extensión.

7.1.8 SINTAXIS Y SEMÁNTICA DE LOS CALIFICADORES DE POLÍTICA

Los certificados pueden contener los calificadores de política *CPS Pointer* y/o *User Notice* con la sintaxis y la semántica especificadas en el estándar IETF RFC 5280.

Los calificadores de políticas contenidos en los certificados se encuentran especificados en las fichas de los perfiles de certificados (ver sección 7.1).

7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA "CERTIFICATE POLICES"

La extensión *Certificate Policies* no está marcada como "crítica" en los certificados, en ningún caso.

7.2 PERFILES DE CRL

Los perfiles de las CRL emitidas por las AC bajo estas DPC cumplen los estándares IETF RFC 5280 e ITU-T X.509.

Las CRL son firmadas por la misma AC que firma los certificados, usando la misma clave privada.

El periodo de validez de las CRL para cada AC se especifica en la sección 4.9.7.

7.2.1 NÚMERO DE VERSIÓN

Todas las CRL son X.509 versión 2.

7.2.2 EXTENSIONES DE CRL Y DE ENTRADA DE CRL

Todas las CRL incluyen las siguientes extensiones de CRL:

- *CRL Number* (OID 2.5.29.20), no crítica, como se define en el estándar IETF RFC 5280.
- *Authority Key Identifier* (OID 2.5.29.35), no crítica, como se define en el estándar IETF RFC 5280.

Las CRL pueden incluir las siguientes extensiones de CRL adicionales:

- *ExpiredCertsOnCRL* (OID 2.5.29.60), no crítica, como se define en el estándar ITU-T X.509, con el valor de fecha y hora en el campo *Validity notBefore* del certificado de la AC.
- *Issuing Distribution Point* (OID 2.5.29), crítica, como se define en el estándar IETF RFC 5280.

Todas las CRL incluyen la siguiente extensión de entrada de CRL:

- *Reason Code* (OID 2.5.29.21), no crítica, como se define en el estándar IETF RFC 5280.

7.3 PERFILES DE OCSP

Los perfiles de las respuestas OCSP cumplen el estándar IETF RFC 6960.

Las respuestas OCSP incluyen el motivo de revocación dentro de la información de cada certificado revocado.

El periodo de validez de las respuestas OCSP para cada AC se especifica en la sección 4.9.10.

El perfil de los certificados OCSP cumple lo especificado en la sección 7.1.

7.3.1 NÚMERO DE VERSIÓN

La versión de las respuestas OCSP es v1, conforme al estándar IETF RFC 6960.

7.3.2 EXTENSIONES OCSP

Las respuestas OCSP incluyen las siguientes extensiones:

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

8 AUDITORÍAS DE CONFORMIDAD

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

Los objetivos de Camerfirma respecto a la seguridad y la calidad han sido fundamentalmente la obtención de la certificación ISO/IEC 27001, ISO/IEC 20000, ISO 9001, ISO 22301, ISO 14001 y ENS, además de la realización de Auditorías internas anuales al sistema de certificación de Camerfirma, y fundamentalmente a las Autoridades de Registro, para garantizar el cumplimiento de los procedimientos internos.

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

Tal y como dispone el Reglamento eIDAS, se comunicará al Organismo de Supervisión cualquier auditoría de la conformidad al menos un mes antes de la previsión de esta, permitiendo la participación del mismo en calidad de observador.

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

Camerfirma está sujeta a una auditoria bienal sobre RGPD y LOPDGDD.

8.1 FRECUENCIA DE LAS AUDITORÍAS

Camerfirma realizará periódicamente las auditorias necesarias. A continuación, se detalla la periodicidad:

- Auditoria ISO 27001, ISO 20000, ISO 9001, ISO 22301, ISO 14001 en ciclos de 3 años con revisiones anuales.
- Auditoría ENS (Esquema Nacional de Seguridad), bienal.
- Evaluación de conformidad con el Reglamento eIDAS, bienal con revisión anual, de acuerdo con el Reglamento eIDAS para los siguientes servicios:
    - *Qualified electronic time stamp*: ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422.
    - *Qualified certificate for electronic signature* (art. 28 del Reglamento eIDAS) : ETSI EN 319 401, ETSI EN 319 411-1 e 411-2, ETSI EN 319 412 (1,2,5).
    - *Qualified certificate for electronic seal* (art. 38 del Reglamento eIDAS): ETSI EN 319 401, ETSI EN 319 411-1 e 411-2, ETSI EN 319 412 (1,2,3,5).
- Auditoria LOPDGDD/RGPD, bienal con revisión anual.
- Un análisis de vulnerabilidades trimestral.

- Un test de intrusión anual.
- Auditorías de AR de forma discrecional.

8.1.1 AUDITORÍAS DE AC SUBORDINADA EXTERNA O CERTIFICACIÓN CRUZADA.

No aplicable.

8.1.2 AUDITORIA EN LAS AR

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

El proceso de auditoría se lleva a cabo realizando un muestreo de certificados emitidos y verificando que se han emitido conforme a las PC de Camerfirma.

8.1.3 AUDITORÍAS INTERNAS

Anualmente, Camerfirma realiza auditorías internas de todas las normas indicadas en el punto 8.1 (control técnico y jurídico).

8.2 IDENTIFICACIÓN Y CUALIFICACIONES DEL AUDITOR

Las auditorías son realizadas por las siguientes compañías externas e independientes. Cuentan con un amplio reconocimiento en seguridad informática, en seguridad de Sistemas de Información y en auditorías de conformidad de Autoridades de Certificación:

- Para las auditorías ISO 27001, ISO 20000, ISO 9001, ISO 22301 - CSQA. https://www.csqa.it
- Para la auditoría ISO 14001 y ENS - CAMARA CERTIFICA. https://www.camaracertifica.es
- Para la evaluación de conformidad con el Reglamento eIDAS Natural Persons & Legal Persons. – CSQA. https://www.csqa.it
- Para la evaluación de conformidad con el Reglamento eIDAS Sellos de tiempo - CSQA. https://www.csqa.it
- Para las auditorías internas y LOPDGDD/RGPD – AUREN https://www.auren.com

8.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Los organismos de evaluación son independientes y de reconocido prestigio, contando con

departamentos especializados en la realización de auditorías informáticas en la gestión de certificados y servicios de confianza, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la AC.

No existe vinculación ni dependencia financiera ni orgánica entre los organismos de evaluación y Camerfirma.

8.4 PUNTOS CUBIERTOS POR LA AUDITORIA

En términos generales, las auditorías verifican:

- Que Camerfirma tiene un sistema que garantiza la calidad del servicio prestado.
- Que Camerfirma cumple con los requisitos de las PC que regulan la emisión de los diferentes tipos de certificados.
- Que Camerfirma gestiona de forma adecuada la seguridad de sus sistemas de información.

Los elementos auditados son:

- Procesos de Camerfirma, AR y elementos relacionados con la emisión de certificados, sellos de tiempo y servicios de validación en línea (OCSP).
- Sistemas de seguridad de la información.
- Protección física y lógica de los centros de procesamiento de datos.
- Documentación requerida para la emisión de cada tipo de certificado.
- Verificación de que los operadores de AR conocen y cumplen la DPC y las PC.

8.5 MEDIDAS TOMADAS COMO RESULTADO DE LAS DEFICIENCIAS

Una vez recibido el informe de evaluación de la auditoría de cumplimiento llevada a cabo, Camerfirma revisará con la entidad que ha ejecutado la auditoría, las deficiencias encontradas y desarrollará y ejecutará un plan de acciones correctivas con objeto de solucionar las deficiencias.

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

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

8.6 COMUNICACIÓN DE RESULTADOS

La comunicación de resultados se realiza al responsable de seguridad y cumplimiento normativo por parte de los auditores que han realizado la evaluación. El certificado de auditoria se publica en la web de Camerfirma.

9 ASPECTOS LEGALES Y OTROS ASUNTOS

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS Y RENOVACIÓN

Los precios de los servicios de certificación o cualquier otro servicio relacionado están disponibles y actualizados en la página Web de Camerfirma https://www.camerfirma.com/certificados-digitales/ o previa consulta al departamento de soporte de Camerfirma en https://www.camerfirma.com/contacto-soporte/ o al teléfono +34 91 136 91 05.

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

9.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a los certificados emitidos es gratuito. Camerfirma implementa controles para evitar los casos de descarga masiva de certificados. Cualquier otra circunstancia que a juicio de Camerfirma deba ser considerada a este respecto se publicara en la página Web de Camerfirma https://www.camerfirma.com/ o previa consulta al departamento de soporte de Camerfirma en https://www.camerfirma.com/contacto-soporte/ o al teléfono +34 91 136 91 05.

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

Camerfirma proporciona un acceso a la información relativa al estado de los certificados o de los certificados revocados a través de CRL y/o mediante OCSP.

Camerfirma proporciona ambos servicios de forma gratuita.

9.1.4 TARIFAS DE OTROS SERVICIOS

El acceso al contenido de estas DPC y PC es gratuito, en la dirección Web de Camerfirma https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/.

9.1.5 POLÍTICA DE REINTEGROS

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

La emisión correcta del certificado sea en el soporte que sea, supone el comienzo de la ejecución

del contrato, con lo que, conforme lo permite la Ley General para la Defensa de los Consumidores y Usuarios (RDL 1/2007) en dichos casos, el Titular pierde su derecho de desistimiento.

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DEL SEGURO

Camerfirma, en su actividad como PSC, dispone de un seguro de responsabilidad civil que contempla sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios: el Titular/Firmante y la Parte que Confía y a terceros, por un importe mínimo de 1.500.000 euros más 500.000 euros por cada tipo de servicio cualificado de los previstos en el Reglamento eIDAS que presta.

Dicho seguro cubre igualmente los servicios que se prestan por las filiales de Camerfirma en el extranjero, considerando como filial la detención por Camerfirma, S.A. de más del 50% de las acciones con derecho a voto o las participaciones.

9.2.2 OTROS ACTIVOS

No estipulado.

9.2.3 SEGURO O COBERTURA DE GARANTÍA PARA ENTIDADES FINALES

Ver apartado 9.2.1.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN DEL NEGOCIO

9.3.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

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

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

9.3.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Camerfirma considera como información no confidencial:

1) La contenida en las presentes DPC y las PC.
2) La información contenida en los certificados.
3) Cualquier información cuya accesibilidad sea prohibida por la normativa vigente.

9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Camerfirma es responsable de la protección de la información confidencial generada o comunicada durante todas las operaciones. Las partes delegadas, como las entidades que administran las AC emisoras Subordinadas o las autoridades de registro, son responsables de proteger la información confidencial que se ha generado o almacenado por sus propios medios.

Para los certificados de entidad final, los Titulares o los Responsables son responsables de proteger su propia clave privada y toda la información de activación (es decir, contraseñas o PIN) necesaria para acceder o usar la clave privada.

9.3.3.1 DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN / SUSPENSIÓN DE CERTIFICADOS

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

Camerfirma dispone de servicios de consulta online de estado de los certificados basados en el estándar OCSP. Los servicios OCSP ofrecen respuestas estandarizadas bajo IETF RFC 6960 sobre el estado de un certificado, es decir, si el certificado consultado está activo, revocado o si ha sido emitido o no por la AC.

9.3.3.2 ENVÍO A LA AUTORIDAD COMPETENTE

Camerfirma proporcionará la información solicitada por la autoridad competente o al organismo regulador correspondiente, en los casos y forma establecidos en la legislación vigente.

9.4 PRIVACIDAD DE LA INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

Camerfirma cumple en todo caso con la normativa vigente en materia de protección de datos, en particular, ha adaptado sus procedimientos al REGLAMENTO (UE) 2016/679 General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

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

9.4.3 INFORMACIÓN NO CONSIDERADA PRIVADA

La información personal sobre un individuo disponible en los contenidos de un certificado o CRL, se considera como no privada al ser necesaria a la prestación del servicio contratado, sin perjuicio de los derechos correspondientes al titular de los datos personales en virtud de la legislación 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 de que sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

No se cederán datos personales a terceros salvo obligación legal.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

Camerfirma es titular de los derechos de propiedad intelectual sobre estas DPC y PC.

9.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL

9.6.1 OBLIGACIONES Y RESPONSABILIDAD DE LA AC

9.6.1.1 AC BAJO ESTA DPC

Pueden consultarse las obligaciones de la AC en el apartado 7 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.1.2 AC SUBORDINADA EXTERNA

No aplicable.

9.6.2 OBLIGACION Y RESPONSABILIDAD DE LA AR

Pueden consultarse las obligaciones de la RA en el apartado 8 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.3 OBLIGACIÓN Y RESPONSABILIDAD DEL SUSCRIPTOR

9.6.3.1 SUSCRIPTOR

Pueden consultarse las obligaciones del suscriptor en el apartado 9 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.3.2 SOLICITANTE

Pueden consultarse las obligaciones del solicitante en el apartado 10 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.3.3 TITULAR Y RESPONSABLE

Pueden consultarse las obligaciones del titular y responsable en el apartado 11 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.3.4 ENTIDAD

En el caso de aquellos certificados que impliquen vinculación a una Entidad, pueden consultarse las obligaciones en el apartado 12 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.4 OBLIGACIÓN Y RESPONSABILIDAD DE LA PARTE QUE CONFÍA

Pueden consultarse las obligaciones y responsabilidades de las partes que confían, en el apartado

13 de los términos y condiciones publicados en el siguiente enlace: https://www.camerfirma.com/condiciones-de-uso-certificados-ac-camerfirma/.

9.6.5 OBLIGACIÓN Y RESPONSABILIDAD DE OTROS PARTICIPANTES

No estipulado.

9.7 EXONERACIÓN DE RESPONSABILIDAD

Según la legislación vigente, la responsabilidad de la AC y de la AR no se extiende a aquellos supuestos en los que la utilización indebida del certificado tiene su origen en conductas imputables al Suscriptor, al Solicitante, al Titular, al Responsable, a la Entidad y a la Parte que Confía por:

- No haber proporcionado información adecuada, inicial o posteriormente como consecuencia de modificaciones de las circunstancias reflejadas en el certificado, cuando su inexactitud no haya podido ser detectada por la AC o la AR.
- Haber incurrido en negligencia con respecto al almacenamiento de la clave privada y a su confidencialidad.
- No haber solicitado la revocación del certificado en caso de duda sobre el mantenimiento de la confidencialidad.
- Haber utilizado la clave privada después de haber expirado el periodo de validez del certificado, o después de que el certificado haya sido revocado, o mientras ha estado suspendido.
- Superar los límites que figuren en el certificado.
- En conductas imputables a la Parte que Confía si éste actúa de forma negligente, es decir cuando no compruebe o tenga en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos y límite de facultades o importe de las transacciones; o cuando no tenga en cuenta el estado de vigencia del certificado.
- De los daños ocasionados al Titular, a la Entidad o a las Partes que Confían por la inexactitud de los datos que consten en el certificado, si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible.
- Un uso inadecuado o fraudulento del certificado en caso de que el Titular y/o, en su caso, el Responsable lo haya cedido o haya autorizado su uso a favor de una tercera persona en virtud de un negocio jurídico como el mandato o apoderamiento, siendo exclusiva responsabilidad del Titular y, en su caso, del Responsable el control de las claves asociadas a su certificado.

Las AC y las AR tampoco serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.

- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente, y estas DPC y PC.
- Por el uso indebido o fraudulento de los certificados, CRL o respuestas OCSP.
- Por el uso de la información contenida en los certificados, CRL o respuestas OCSP.
- Por el perjuicio causado en el periodo de verificación de los motivos de revocación.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Titular.

9.8 LIMITACIÓN DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

El límite monetario del valor de las transacciones se puede expresar en el propio certificado de entidad final mediante la inclusión del correspondiente *QCStatement* en la extensión *Qualified Certificate Statements*, conforme a lo dispuesto en el estándar ETSI EN 319 412-5.

Si la extensión del certificado anteriormente expuesta no lo contradice, el límite máximo que Camerfirma permite en las transacciones económicas realizadas es de 0 (cero) euros. No obstante, el suscriptor y las terceras partes pueden establecer acuerdos o coberturas específicas de manera bilateral para transacciones de mayor valor. En estos casos, se mantendrá el límite de responsabilidad de la CA mencionado en los párrafos anteriores, conforme a la política de certificación aplicable.

9.9 INDEMNIZACIONES

Ver apartado 9.2 y 9.6.1.

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

Ver apartado 5.8.

Esta DPC así como las PC y las PDS entrarán en vigor en el momento de su publicación en la web de Camerfirma.

9.10.2 FINALIZACIÓN

Ver apartado 5.8.

Esta versión de la DPC así como las versiones actuales de las PC y las PDS serán derogadas y sustituidas por la nueva versión en el momento de su publicación. Las nuevas versiones sustituyen

totalmente a su versión anterior.

9.10.3 EFECTO DE LA TERMINACIÓN Y SUPERVIVENCIA

Ver apartado 5.8.

9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

Cualquier notificación referente a las presentes DPC y PC se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado 1.5.2.

9.12 MODIFICACIONES

9.12.1 PROCEDIMIENTO DE MODIFICACIÓN

La AC se reserva el derecho de modificar este documento por razones técnicas o para reflejar cualquier cambio en los procedimientos que se hayan producido debido a requisitos legales, reglamentarios (Reglamento eIDAS, CA/Browser Forum, Organismos de Supervisión Nacional, etc.) o como resultado de la optimización del ciclo de trabajo. Cada nueva versión de estas DPC y PC reemplaza a todas las versiones anteriores, que siguen siendo, sin embargo, aplicables a los certificados emitidos mientras esas versiones estaban vigentes. Se publicará al menos una actualización anual. Estas actualizaciones quedaran reflejadas en el cuadro de versiones al final del documento.

Los cambios que pueden realizarse a estas DPC y las PC no requieren notificación excepto que afecte de forma directa a los derechos de los Suscriptores o los Titulares de los certificados, en cuyo caso podrán presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

9.12.2 MECANISMO DE NOTIFICACIÓN Y PLAZOS

9.12.2.1 LISTA DE ELEMENTOS

Cualquier elemento de esta DPC y las PC puede ser cambiado sin preaviso.

9.12.2.2 MECANISMO DE NOTIFICACIÓN

Todos los cambios propuestos de esta DPC y las PC serán inmediatamente publicados en la web de Camerfirma https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

En este mismo documento existe un apartado de cambios y versiones donde se puede conocer los cambios producidos desde su creación y la fecha de dichas modificaciones.

Los cambios de este documento se comunican a aquellos organismos y empresas terceras que emiten certificados bajo estas DPC y/o PC. Especialmente se notificarán los cambios en estas DPC y PC al Organismo de Supervisión nacional.

9.12.2.3 *PERIODO DE COMENTARIOS*

Los Suscriptores y los Titulares afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la recepción de la notificación.

9.12.2.4 *MECANISMO DE TRATAMIENTO DE LOS COMENTARIOS*

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

9.12.3 CIRCUNSTANCIAS EN LAS QUE SE DEBE CAMBIAR EL OID

No estipulado.

9.13 PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

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

9.14 LEGISLACIÓN APLICABLE

La ejecución, interpretación, modificación o validez de las presentes DPC y las PC se regirá por lo dispuesto en la legislación española y de la Unión Europea vigente en cada momento. En concreto, esta DPC y las PC se rigen por la siguiente normativa:

- Reglamento (UE) 910/2014, del Parlamento 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 modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (Reglamento eIDAS).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y

la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2), (NIS2).

- Reglamento de Ejecución (UE) 2024/2690, de 17 de octubre de 2024, por el que se establecen disposiciones de aplicación de la Directiva (UE) 2022/2555 en los requisitos técnicos y metodológicos de las medidas de gestión de riesgos en materia de ciberseguridad y una mayor especificación de los casos en que un incidente se considera significativo con los proveedores de servicios de confianza y otros sujetos obligados.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Reglamento (UE) 2016/679, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados
- Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

9.15 CONFORMIDAD CON LA LEY APLICABLE

Ver apartado 9.14.

9.16 CLÁUSULAS DIVERSAS

9.16.1 ACUERDO COMPLETO

Las partes de esta DPC y las PC asumen en su totalidad el contenido de este documento.

9.16.2 ASIGNACIÓN

Las partes de estas DPC y las PC no pueden ceder ninguno de sus derechos u obligaciones bajo estas DPC y PC o acuerdos aplicables sin el consentimiento por escrito de Camerfirma.

9.16.3 SEPARABILIDAD

Si las disposiciones individuales de estas DPC y las PC 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 estas DPC y PC, 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 estas DPC y las PC no elimina el derecho de Camerfirma de hacer cumplir las mismas disposiciones más adelante o el derecho de hacer cumplir cualquier otra disposición de estas DPC y PC. Para ser efectiva, cualquier renuncia debe estar por escrito y firmada por Camerfirma.

9.16.5 FUERZA MAYOR

Las cláusulas de fuerza mayor, si existen, están incluidas en el "Acuerdo del suscriptor".

9.17 OTRAS PROVISIONES

No estipulado.

Apendice 1 Historia del documento

May 2016	V1.0	Adaptación EIDAS
Nov 2016	V1.1	Modificaciones realizadas en el proceso de evaluación de conformidad.
Mar 2017	V1.2	Ampliación de estructuras de CA, revisión y modificaciones perfiles de certificados.
Abr 2017	V1.2.1	Incorporación de las comprobaciones CAA en certificados de Servidor Seguro y Sedes electrónicas según RFC 6844.
Feb 2018	V1.2.2	1.2 aclaración sobre el alineamiento de estas prácticas con los *Baseline Requirement* de CA/Browser Forum (punto 1.1 después de adaptación a estructura RFC3647) 1.2.1.3 -Correcciones OIDs de los certificados de EP con PSEUDÓNIMO (punto 1.3.11.3 después de adaptación a estructura RFC3647) 1.2.1.3.4 - Aclaración duración de los certificados de TSU y aceptación de las practicas por parte del suscriptor con dispositivo TSU homologado. (punto 1.3.11.3.4 después de adaptación a estructura RFC3647) 1.2.1.4.3 - Incorporación de la fecha de despliegue de Camerfirma Perú (punto 1.3.11.4.1.7 después de adaptación a estructura RFC3647) 1.5.5 - Incorporación de la figura de Agencia delegada para Camerfirma Perú (punto 1.3.2 después de adaptación a estructura RFC3647) 4.8.3 Revocación por parte de terceros. Revocación en caso de una incorrecta emisión (Requisito CA/Browser Forum). (punto 4.9.2 después de adaptación a estructura RFC3647).
Mar 2018	V1.2.3	1.5.5 Las RA para SSL no pueden validar el dominio. CA/Browser Forum. (punto 1.3.2 después de adaptación a estructura RFC3647) 2.5.3 Aclaración servicio gratuito OCSP. (punto 9.1.3 después de adaptación a estructura RFC3647) 2.1.5 responsabilidad usuario - Comprobación TSL (punto 9.6.4 después de adaptación a estructura RFC3647)
May 2018	V1.2.4	1.3.3, 1.3.9 y 1.3.10 Aclaraciones conceptos Sujeto/Titular y Firmante/Creador del sello y Solicitante y Responsable del certificado. 3.2.3.1 Otros documentos aceptados para acreditar la vinculación entre el titular del dominio y el titular del certificado.

		9.1.5 Modificación política de reintegros 9.4 Actualización de la cláusula sobre privacidad de la información personal conforme RGPD 9.7 Exoneración de responsabilidad de la AC y AR en caso de delegación del certificado a un tercero Adaptación de la estructura del documento CPS en base a la RFC3647 1.3.11.3 Incorporación de jerarquía CHAMBERS OF COMMERCE ROOT - 2018 1.3.11.4 Incorporación de CA subordinada AC CAMERFIRMA GLOBAL TSA – 2018
Jun 2018	V1.2.5	Corrección nomenclatura de dispositivo seguro a dispositivo cualificado. Corrección de direcciones URL por cambio de página web de Camerfirma. Incorporación de la CA CN = Camerfirma Corporate Server II – 2015 como CA cualificada. 3.2.1 Almacenamiento de claves generadas por Camerfirma y almacenadas remotamente. 3.2.3.2 Correcciones. 3.2.3.4 Eliminado 3.2.3.4 Consideraciones en la identificación usuarios y vinculación en al AAPP. 3.3.2 Incorporación de texto explicativo adicional. 4.1.2.5 Modificación certificación cruzada. 8.1.1 Corrección requisitos para organizaciones con certificados de SubCA o Certificación cruzada de Camerfirma. 8.2 Actualización auditores eIDAS.
Jul 2018	V1.2.6	1.3.11.4.1.4 Cambio en la duración de los años de certificados cualificados de TSU a 5 años como máximo. 8.7 Aclaración auditoría interna sobre el 3% de los certificados SSL/TSL 9.12.2.2 Notificaciones a los Supervisores Nacionales ES, PE, CO, MX
Sep 2018	V1.2.7	Cambio de orden, denominación y desarrollo en diversos puntos para alinear con RFC3647 Se desarrolla el punto '9.12.1 Procedimiento de modificación'

Sep 2018	V1.2.8	3.2.5.1 Identificación de la vinculación, se declara que la validación de los dominios se realizará por uno de los métodos aceptados por CA/Browser Forum Declaración de la versión de *Guidelines For The Issuance And Management Of Extended Validation Certificates* elaborado por el CA/Browser Forum con las que están alineadas estas CPS
Sep 2018	V1.2.9	cambios menores en el formato del documento 3.2.5.1 Identificación de la vinculación. Declaración explicita de los métodos utilizados. 3.2.3 Incorporación del procedimiento de comprobación de control sobre la cuenta de email del solicitante. 4.2.1 Se incluyen las comprobaciones sobre CAA anteriormente declaradas en 3.2.5.2 Se retira la Jerarquía CHAMBERS OF COMMERCE ROOT – 2018 9.16.4 actualizado 6.2.3 actualizado
Feb 2019	V1.2.10	1.3.2 Modificación y aclaración del concepto de Agencia Delegada en la CA Camerfirma Perú y se retira que las Empresas españolas puedan ser RAs de las CAs: AC CAMERFIRMA FOR WEBSITES-2016, AC CAMERFIRMA GLOBAL FOR WEBSITES-2016 y CAMERFIRMA CORPORATE SERVER II – 2015 1.3.2 Se incluye la jerarquía CHAMBERS OF COMMERCE ROOT 2018 1.3.5.7.3.1 se sustituye la jerarquía de 2016 por la de 2018 1.3.5.7.3.5 AC CAMERFIRMA FOR NATURAL PERSONS. (Certificados para personas físicas) 1.4.1 Usos apropiados de los certificados 1.4.2 Usos prohibidos y no autorizados de los certificados 1.6.2 Definición de Firma remota y Sello remoto 2.2.1 Políticas y Prácticas de Certificación. 2.2.2 Términos y condiciones. 3.1.3 Quitar referencia a políticas. 3.1.5.1 Emisión de varios certificados de persona física para un mismo titular 3.1.6 Reconocimiento, autenticación y función de marcas registradas y otros signos distintivos

		3.2.1 Métodos de prueba de la posesión de la clave privada y referencia a lista de QSCD. 3.2.2.1 Identidad 3.2.3 Identificación de la identidad de un individuo. 3.2.2.5 registro IP URL 3.4 Identificación y autenticación de una solicitud de revocación 4.1.2.4 eliminación referencia políticas 4.1.2.5 Notas certificación cruzada 4.2.2 aclaración entrega documentación y acceso WS 4.2.3 Plazo SubCAs no estipulado 4..3.1.3 Solicitudes WS autenticadas. 4.5.1 Uso del certificado y la clave privada del suscriptor, se incluyen condiciones de uso para firma remota y sello remoto 4.5.1 Se incluye la jerarquía CHAMBERS OF COMMERCE ROOT 2018 4.6.1 No renovaciones certificados de componente. 4.9.2 Eliminar referencia a políticas. 4.9.5 Aclaración revocación 4.12.1 Incorporación de custodia de claves en dispositivo en nube. 5.2.1 Eliminar referencia políticas 5.3.1 Eliminar documento de referencia 5.5.1 Custodia de los eventos relacionados con la plataforma de gestión centralizada de claves. 5.7 Eliminar documento de referencia 5.7.4 Eliminar referencia temporal 6.1.1 Se incluye la jerarquía CHAMBERS OF COMMERCE ROOT 2018 6.1.1.1 Incluir tratamiento onbehalf 6.2.1.2 error en documento de referencia pasar a 6.2.1.1 – Incluir Onbehalf 6.2.3 Incluir tratamiento onbehalf 6.2.4 Incluir tratamiento onbehalf 6.2.6 Incluir tratamiento onbehalf 6.2.7 Incluir tratamiento onbehalf

		6.2.8 Incluir tratamiento onbehalf 6.2.9 Incluir tratamiento onbehalf 6.2.10 Incluir tratamiento onbehalf 6.2.11 Incluir tratamiento onbehalf 6.4 Activación de datos de firma en plataforma centralizada. 6.4.2 Incluir tratamiento onbehalf 6.6 Gestión del ciclo de vida en plataforma centralizada. 9.6.4 Se advierte de la responsabilidad del Firmante/Creador del sello y del Sujeto/Titular en caso de delegación de uso de certificados a terceras personas 9.6.5 Obligación y responsabilidad de terceras partes, se detallan las obligaciones de certificados de Representante de Persona Jurídica 9.6.1.1 Incorporación de responsabilidad de la AC respecto a las claves almacenadas de forma centralizada. 9.6.2 Obligación y responsabilidad de la RA 9.6.4.1 y 9.6.4.2 Aclara responsabilidad del Sujeto/Titular y del Firmante/Creador del sello respecto a sus obligaciones de custodia de los datos de activación de la clave privada 9.7 Exoneración de responsabilidad 9.12.2.2 Comunicación cambios a los auditores
Enero 2020	V1.2.11	1.3.1 Incorpora datos corporativos de AC Camerfirma SA y su participación por InfoCert, S.p.A. 1.3.2 Adición de requisitos para emisión de certificados a no residentes en España y para autorización de RA externas que emitan certificados de Servidor Seguro. 1.3.5.1 Sustituye en todo el documento el término “SubCA” por “AC intermedia” y su sujeción a la CPS de la CA Raíz 1.3.5.7 Se aclara que la CPS recoge las jerarquías y CAs gestionadas por Camerfirma como propietaria, remitiendo a las CPS de las CAs propietarias de otras organizaciones. 1.3.5.7.3 Actualización de la **Jerarquía CHAMBERS OF COMMERCE**: - revocación de la Root “CHAMBERS OF COMMERCE ROOT - 2018” y su AC intermedia “AC CAMERFIRMA FOR WEBSITES 2018” - revocación de AC intermedia “AC CAMERFIRMA CODESIGN – 2016”

		(bajo “CHAMBERS OF COMMERCE ROOT – 2016”) - creación de AC intermedia “IVSIGN CA” (CPS propia bajo CHAMBERS OF COMMERCE ROOT -2016”) 1.3.5.7.3.2 Se aclara cómo se generan y almacenan las claves 1.3.5.7.3.5.2.1 Aclaraciones de las funcionalidades de los Certificados Cualificados de Representante Legal, 1.3.5.7.4 Actualización de la **Jerarquía GLOBAL CHAMBERSIGN ROOT – 2016:** - revocación de la AC intermedia “AC CAMERFIRMA – 2016” y todas sus AC intermedias segundo nivel - revocación de la AC intermedia segundo nivel “AC CITISEG – 2016” (bajo la AC intermedia “AC CAMERFIRMA COLOMBIA – 2016”) - creación de las AC intermedias segundo nivel “CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 001” y “CAMERFIRMA COLOMBIA SAS CERTIFICADOS – 002” (bajo la AC intermedia “AC CAMERFIRMA COLOMBIA – 2016”) 2.3 Se incorpora periodicidad de versión de CPS 3.2.2.1 En la identificación de la entidad para certificados SSL EV, se debe comprobar la categoría de entidad según las políticas de CA/Browser Forum 3.2.3 Se detallan los métodos alternativos de identificación de un individuo según recoge el Reglamento eIDAS en art. 24.1 y se indica que la comprobación del control del correo electrónico se hace exclusivamente por la CA 4.5.1 Se actualiza el cuadro de uso de clave con las CA vigentes 4.9 Se precisa donde consultar los certificados caducados y no caducados y durante cuánto tiempo en caso de revocación de CA intermedia 4.9.1 Se añade 2 causas de revocación alineadas con Mozilla Root Store Policy 4.9.7 Se actualiza el cuadro de frecuencia de emisión CRL con las CA vigentes 6.1.1 Se actualiza el cuadro sobre generación del par de claves con las CA vigentes 6.1.7 Se indica explícitamente que las claves de roots no emiten certificados de entidad final (salvo los respondedores OCSP) 6.2.11 Control de la cualificación de dispositivos y actuaciones en

		caso de su perdida 8.1.3 Aclaración frecuencia auditorías internas y volumen para SSL
Mayo 2020	V1.2.12	1.3.2 Cambio de control donde decía posesión del dominio. 1.3.5.7.3 Jerarquía CHAMBER OF COMMERCE: se incorpora la jerarquía CHAMBERS OF COMMERCE ROOT y AC intermedia "AC CAMERFIRMA CERTIFICADOS CAMERALES" 1.3.5.7.3.3 Se elimina información de Certificados de Firma de Código (AC CAMERFIRMA CODESIGN – 2016 revocada) 1.3.5.7.4 Jerarquía GLOBAL CHAMBERSIGN ROOT: se añaden los OIDs de la CA intermedia "AC CAMERFIRMA PERÚ CERTIFICADOS – PERÚ" en soporte Hardware (adaptación Guía EC v.4.1 INDECOPI) 3.2.3 Identificación de la identidad de un individuo: nueva redacción para incorporar todos los métodos de identificación previsto por el Reglamento eIDAS y normas nacionales 3.2.5.1 Se añade referencia a la conservación de la información y documentación de datos de emisión, en soporte físico o por medios electrónicos. Eliminación del requerimiento de evidencia titularidad del dominio. 4.5.1 Se actualiza el cuadro de uso de clave con las CA vigentes 4.9.7 Se actualiza el cuadro de frecuencia de emisión CRL con las CA vigentes 5.2.1 Se precisa que un Operador de RA no puede emitirse un certificado a sí mismo 6.1.1 Se actualiza el cuadro sobre generación del par de claves con las CA vigentes 7.3 Se precisa las especificaciones del perfil de mensajes OCSP 8.1 Se elimina las referencias a Auditorias WebTrust y se detallan las normas ETSI sobre las que se basa la auditoria eIDAS 8.2 Se actualiza la identificación de auditorías y auditores
Enero 2021	V1.2.13	Incorporación de OIDs 1.3.5.7.3 y 1.3.7.5.4
Febrero 2021	V1.2.14	3.2.1.1 Incorporación de Agencias de Registro 4.3.1.4 Incorporación de política de firma ETSI TS 119 431-2 4.6.1 Modificación del periodo de uso de clave de un certificado de TSU.

		5.4.3 Actualización periodo retención de logs.
Marzo 2021	V1.2.15	1.1 (y resto del documento) se elimina la referencia a la Ley 59/2003 y se añade referencia a la Ley 6/2020. 1.3.5.7.3, 1.3.5.7.3.4.1.2, 1.3.5.7.3.4.1.3 Con el mismo OID, se incorporan nuevos certificados de Autónomo y de Autónomo colegiado. 1.3.5.7.3.4.2 Aclaraciones sobre las facultades de los Representantes y cómo acreditarlas. 1.3.5.7.4.2.1 Aclaraciones sobre el nombre de los perfiles de certificados bajo la AC CAMERFIRMA PERÚ para su adecuación a las Guías de INDECOPI 1.4.1 y 1.4.2 Aclaraciones sobre usos apropiados de los certificados y usos prohibidos 3.2.5.1 Se añade información sobre la 'Documentación' acreditativa de los certificados de Autónomo y Autónomo Colegiado 3.3.1 Aclaración en la redacción de la validación para la renovación de certificado y puesta en conformidad con Ley 6/2020 En todo el documento: modificación de las URL que remiten a la página web de Camerfirma tras lanzamiento de nueva web con cambio de estructura de la información.
Abril 2021	V1.2.16	1.3.5.7.4.2 Extensión del ámbito geográfico de la AC Camerfirma Perú a LATAM 4.9.12 Inclusión de instrucciones para notificar compromiso de la clave privada.
Julio 2021	V1.2.17	Retirada de esta CPS de AC CAMERFIRMA FOR WEBSITES 2016 y CAMERFIRMA CORPORATE SERVER 2015 II y de los requisitos y detalles de los certificados de website 1.3.5.7.3 Incluir perfiles y OID de CamerCloud 1.3.5.7.3.2.2 Se indica el punto en el que estarán disponibles los distintos certificados de TSU. 1.6.1 Incorporación de nuevos acrónimos 3.2.3 Sustitución de 'no UE ni EEE' por 'de otros países' 3.2.3 Ampliación de información acerca de VideoID e incorporación de SelfID 4.3.1.4 Incorporación de requisitos de los certificados

		ManagedOnBehalf 4.4.3.1 Incorporación del OID de la política para la identificación de certificados generados en dispositivos no certificados de creación de firma o de creación de sello. 6.2.8,6.2.9,6.2.10,.4.2 Ampliación de información detallada para certificados en CKC.
Octubre 2021	V1.2.18	1.1 Visión General: Se añade presentación general de Camerfirma Perú, S.A.C., referencias a la normativa que le es aplicable y los servicios que brinda bajo acreditación de INDECOPI. Se informa que la presente DPC aplica a la AC Camerfirma Perú Certificados – 2016 salvo que se indique expresamente que "No aplica a AC Perú" o "Aplica solo a AC Perú". 1.3.1 Se añaden datos corporativos y de contacto de Camerfirma Perú, S.A.C. como Autoridad de Certificación. 1.3.2 En la descripción de los tipos de Autoridades de Registro, se añade referencia a la Entidad de Registro (ER) de Camerfirma Perú S.A.C. y las ER externas. Se elimina cuadro resumen. 1.3.3 Se añade definición del "Titular" del certificado según normativa peruana. 1.3.5.2 Se añade referencia a la Autoridad Administrativa Competente en Perú (INDECOPI) 1.3.5.4 Se añade definición de la "Entidad" en los certificados de sellos electrónico. 1.3.5.5 Se añade definición del "Solicitante" y "Suscriptor" del certificado según normativa peruana. 1.3.5.6 Se añade definición del "Responsable" del certificado según normativa peruana. 1.3.5.7.4. y 1.3.5.7.4.2 AC Camerfirma Perú Certificados - 2016. Modificación de la denominación de varios perfiles para ajustarlos a la denominación utilizada en el marco legal peruano aplicable a la firma y certificados digitales y las Guías de acreditación de INDECOPI. Incorporación del perfil de Certificado de Sello Electrónico de Empresa en Panamá y del perfil de Certificado de Persona Natural – Profesional Colegiado 1.4.2 Se considera usos prohibidos y no autorizados, los que determina la normativa peruana. 1.6.1 Se añaden acrónimos de EC y ER 1.6.2 Se amplían definiciones de Autoridad de Certificación y

		Autoridad de Registro para incorporar las Entidades de Certificación y Entidades de Registro según terminología peruana. 2.1 y 2.2 Se añade al Repositorio, vínculos a servicios de la web de Camerfirma Perú. 3.1.1 Se modifica número de teléfono de contacto y se elimina referencia a estructura y contenido del certificado de servidor. 3.2.2.1 Se añade que la AC de Perú podrá usar el Registro Mercantil de Panamá para identificar las entidades. 3.2.3 Se añade referencia a los documentos de identidad de un individuo nacional o residente en Perú. 3.3 Aclaración conceptual y terminológica aplicable a AC Perú acerca de la "reemisión" de certificados. 4.5.1 Se añaden nuevos perfiles en cuadro de uso del certificado y clave privada del suscriptor. 4.6.1 Se añaden circunstancias específicas de las reemisiones de certificados bajo la AC Perú, aunque se indica que actualmente no se ofrece el servicio. 4.6.7 Se elimina párrafo sobre certificado TSL. 5.7.1 Se precisa que no se emitirán certificados mientras persista un incidente de compromiso de clave privada de la AC. 5.8 Se añaden actuaciones en caso de cese de la AC o AR para adecuar a requisitos de normativa peruana. 8. En todo el apartado, se añade referencia a las auditorias que aplican a servicios brindados en Perú. 9. Se precisa donde encontrar las tarifas y política de reembolso de los servicios brindados en Perú. 9.2.1 Modificación de los importes cubiertos por el Seguro conforme a la Ley 6/2020 e indicación que la Póliza debe cubrir los servicios de las filiales.
Noviembre 2021	V1.2.19	1.3.5.2 Se actualiza la declaración del organismo de supervisión nacional dentro del Estado Español. 1.3.5.7.3 Se incluye la root 'Chambers of Commerce Root - 2008'. 1.3.5.7.3 Se incorpora información adicional acerca de los dispositivos donde se generan las claves. 1.3.5.7.3 Se especifica si los OIDs de las políticas existentes se corresponden con generados y almacenados en dispositivos QSCD Tarjeta/Token, QSCD Nube o No QSCD (Software, Nube o Dispositivo

		Externo). 1.3.5.7.3 Se retiran de esta tabla los certificados de Sello Electrónico emitidos por Camerfirma AAPP II - 2014. 1.3.5.7.3.1.1 Se retira una declaración y se incorpora dicha declaración al punto 1.3.5.7.3 1.3.5.7.3.3 Incorporar aclaración de los OIDs incorporados a los certificados emitidos en dispositivos cualificados y no cualificados. 3.2.1 Mejora en la información suministrada acerca de los distintos métodos de prueba de posesión de clave privada. 3.2.3 Aclaraciones relacionadas con los métodos de identificación e incorporación de la referencia al proceso asistido con pre-validación de documentación. 3.3 Corrección en el nombre de la CA. 4.1.2.1 Corrección del PKCS utilizado y declaración extendida. 4.3.1.4 Se incorporan aclaraciones acerca de los OIDs incorporados a los certificados. 4.9.11 Sustitución de la página web referenciada. 4.12.1 Declaración de que pueden ser dispositivos cualificados y no cualificados. 4.12.1, 5.5.1, 6.2.4, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10, 6.4.2, 9.6.1.1 Sustitución del término CKC por 'cualificado o no cualificado'. 6.1.1.1 Reformulación del párrafo donde se referenciaba a los CKC. 6.2.1.2 Se amplía información acerca de generación en la plataforma centralizada y de las comprobaciones que Camerfirma realiza. 6.2.3 Se incorpora la excepción de las claves generadas en plataformas centralizadas gestionadas por Camerfirma. 6.2.11 Se amplía información acerca de generación en la plataforma centralizada. 9.12.2.2 Sustitución de Ministerio de Economía y Empresa por Organismo de supervisión nacional.
17/05/2022	V1.2.20	Se actualiza el formato del documento y se añade un código de documento. Se incorpora la posibilidad de generar claves en dispositivos no cualificados (tarjetas y tokens). Se actualizan los nombres de los perfiles de certificados cualificados emitidos por las CAs que aparecen en esta CPS para definir mejor su

		naturaleza. Se actualizan todas las referencias a la plataforma STATUS como Camerfirma STATUS® 1.3.1 Se incorpora el contenido del punto 1.3.5.1 de la versión anterior. 1.3.5.7 se traslada su contenido a 1.3.1.1. 1.5 Se actualiza su contenido. Se sustituye el término 'hardware' por 'Tarjeta/Token' en los casos que se considera necesario. 1.3.1.1.3.3.2.5 y 1.3.1.1.3.3.2.6 se actualiza su redacción. 1.3.5.7.3.2.2 Se eliminan los certificados de TSU. 4.4.3 pasa a estar no estipulado. 5.2.1 Se elimina la incompatibilidad entre el rol Administrador de CA y Operador de CA. 5.4.3 Se incrementa el periodo de conservación de los registros de auditoría. 5.7 Se actualiza su contenido. 5.8 Se actualiza el contenido del punto. 6.6.2 Se actualiza la distribución del contenido del punto. Cambios menores en la redacción del documento. Se actualiza en la portada del documento los datos de creación, verificación y aprobación de esta CPS.
15/07/2022	V1.3.0	El presente documento cambia su nombre de "DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA EIDAS" a "DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CAMERFIRMA 2003-2008-2016". Este documento da continuidad al documento "DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA EIDAS V1.2.20", incorporando el contenido vigente del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA (Certificados No Cualificados) V3.3.7". Estos documentos, así como las versiones anteriores de los mismos pueden ser consultadas en https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/practicas-de-certificacion-ac-camerfirma-cps-dpc-versiones-anteriores/

		Cambios menores en el estilo y la puntuación del documento. 1.1 Actualización de versión de la referencia a la norma EN 319 401 y contenido adicional 1.3.1 Autoridades de Certificación. Cambios generales. 3.2.3 Identificación de la identidad de un individuo. Mayor concreción en los métodos de identificación 2 y 3. 3.2.5.1 Identificación de la vinculación. Incorporación de los certificados de firma de código. 4.5.1 Uso del certificado y la clave privada del suscriptor. Incorporación de los casos añadidos al punto '1.3.1 Autoridades ce Certificación' en esta versión de este documento. 4.9.3 Procedimiento de solicitud de revocación. Actualización de los procedimientos. 4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación. Establecimiento de un límite de 24 horas desde que se recibe la solicitud de revocación hasta que se publica la revocación. 4.9.7 Frecuencia de emisión de CRL. Incorporación de los casos añadidos al punto '1.3.1 Autoridades ce Certificación' en esta versión de este documento. 6.1.1 Generación del par de claves. Incorporación de los casos añadidos al punto '1.3.1 Autoridades ce Certificación' en esta versión de este documento. 7.1.3 Identificadores de objeto (OID) de los algoritmos. Incorporación del algoritmo sha1WithRSAEncryption.
23/08/2022	V1.3.1	1.3.1.2, 3.2.5.1, 4.5.1, sustitución de la denominación en la jerarquía 'AC CAMERFIRMA PERÚ CERTIFICADOS – 2016' de los perfiles de 'Certificado de Persona Natural Profesional Colegiado' por 'Certificado de Persona Jurídica - Atributo Profesional Colegiado' 1.3.1.2.2.1.8 Certificado de Persona Jurídica - Atributo Profesional Colegiado, reformulación del texto que describe este perfil. 1.3.2 AUTORIDADES DE REGISTRO (RA), sustitución de 'Agencia Delegada' por 'Sucursal'. 1.6.1 ACRÓNIMOS, 5.1.1 UBICACIÓN Y CONSTRUCCIÓN, 5.1.2 ACCESO FÍSICO, el servicio de OCSP se ofrece desde la nube de AWS. 4.9.2 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN, incorporación de la posibilidad de solicitud revocación a través de un sello electrónico basado en un certificado emitido por Camerfirma a nombre de la

		Entidad. 4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN, incorporación de mecanismo de revocación a través de servicio web. 5.4.3 PERIODOS DE RETENCIÓN PARA LOS REGISTROS DE AUDITORIA, reducción del periodo de retención de 20 a 15 años. Cambios menores en la redacción del documento. Apéndice I: historia del documento, incorporación de la fecha de firma de este documento en su versión 1.3.0
31/03/2023	V1.4.0	El documento cambia su nombre de "Declaración de Prácticas de Certificación CAMERFIRMA 2003-2008-2016" a "Declaración de Prácticas de Certificación y Políticas de Certificación CAMERFIRMA 2008-2016". Esta versión especifica la DPC de Camerfirma y Camerfirma Perú y las PC de Camerfirma para las AC activas de Camerfirma y Camerfirma Perú bajo las jerarquías de Camerfirma de 2008 y 2016 (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, Global Chambersign Root – 2008, GLOBAL CHAMBERSIGN ROOT – 2016). Se actualiza el formato del documento. Se corrige el código del documento en la portada (está mal en las versiones 1.3.0 y 1.3.1). Se eliminan las siguientes AC terminadas, conforme a lo especificado en la sección 5.8.2 de esta versión, y sus PC: - Jerarquía CHAMBERS OF COMMERCE ROOT – 2016: AC CAMERFIRMA FOR WEBSITES – 2016 (esta AC no está incluida en las versiones 1.3.0 y 1.3.1 pero debería estar; aunque no tenía certificados emitidos activos, aún no estaba terminada). - Jerarquía Chambers of Commerce Root (jerarquía de Camerfirma de 2003, sin AC activas): AC Camerfirma Express Corporate Server, AC Camerfirma Certificados Camerales, Chambers of Commerce Root. - Jerarquía Global Chambersign Root – 2008: AC CAMERFIRMA – 2009, Entitat de Certificació de l'Administració Pública Andorrana-19, MULTICERT SSL Certification Authority 001, DigitalSign Primary CA, DigitalSign CA, DigitalSign TSA. - Jerarquía Global Chambersign Root (jerarquía de Camerfirma de 2003, sin AC activas): RACER, AC Camerfirma, Global Chambersign Root.

		Se eliminan las siguientes PC terminadas (sin certificados activos) de AC activas: - AC CAMERFIRMA AAPP II – 2014: 1.3.6.1.4.1.17326.1.3.3.1, 1.3.6.1.4.1.17326.1.3.4.1, 1.3.6.1.4.1.17326.1.3.4.2, 1.3.6.1.4.1.17326.1.3.4.3 Se incluyen las siguientes PC activas de AC activas, que no están incluidas en las versiones 1.3.0 y 1.3.1 pero deberían estar; aunque las AC no emiten nuevos certificados bajo estas PC, aún existen certificados activos emitidos por las AC bajo estas PC próximos a expirar: - Camerfirma TSA II – 2014: 1.3.6.1.4.1.17326.10.13.1.2 (Certificado No Cualificado de TSU - P12). - Camerfirma TSA – 2013: 1.3.6.1.4.1.17326.10.13.1.3 (Certificado No Cualificado de TSU - HSM). Revisión y homogeneización de términos y siglas. Se eliminan las referencias a documentos internos de Camerfirma. 1.1. Revisión. 1.2. Actualización. Se cambian el nombre y la descripción del documento. Se incluyen los OID de Camerfirma de las PC activas de las AC de Camerfirma bajo las jerarquías de Camerfirma de 2008 y 2016. 1.3 y todas sus secciones. Revisión y actualización. 1.3.1.1, 1.3.1.2. Todas las AC que operan bajo estas jerarquías lo hacen desde infraestructuras controladas técnicamente por Camerfirma. Actualización de AC y PC. 1.3.1.1 y sus secciones, 1.3.1.2 y sus secciones. Se añaden más datos de identificación de los certificados de AC Raíz activas de las jerarquías. Se añaden los datos de identificación de los certificados de las AC Subordinadas bajo esta DPC dentro de las jerarquías. 1.3.1.3 Certificados OCSP. Nueva sección. 1.3.1.5. La AC CAMERFIRMA GESTIÓN INTERNA está fuera del alcance de estas DPC y PC. 1.3.2 AR. Nuevo PVR (Punto de Verificación Remota). 1.3.3 Suscriptores. Se incorporan secciones que estaban en la sección 1.3.5 Otros participantes. Cambio en nombres de participantes. Se añade el participante Suscriptor. 1..4.1, 1.4.2. Revisión. 1.6.1, 1.6.2. Revisión y actualización. Cambio de orden de las

		secciones. 2 todas sus secciones. Revisión y actualización. Cambios en sitios y direcciones web. Cambios en la información publicada. 3 y todas sus secciones. Revisión y actualización. Eliminación de las secciones 3.1.5.1, 3.2.5.3 y 3.2.5.4. 3.2.3. Se elimina como proceso de identificación remota por vídeo, el proceso asistido con pre-validación de documentación y mediación síncrona de un operador. Se añade la descripción métodos alternativos de comprobación de la identidad del Solicitante para certificados no cualificados. 4 y todas sus secciones. Revisión y actualización. 4.4.2. La AC no hará públicos los certificados de entidad final, con excepción de los certificados de TSU propiedad de Camerfirma. 4.4.3. Se añade la notificación a otras entidades de certificados de TSU, OCSP, AC Raíces y AC Subordinadas. 4.5.1. Actualización de AC y PC. 4.6, 4.7. Se mueve el contenido de la sección 4.6 a la sección 4.7. Se añade la descripción del proceso de renovación de un certificado con cambio de claves en casos de sustitución del certificado. 4.9.1. Nuevas circunstancias para la revocación. 4.9.2. Cambios en quién puede solicitar la revocación. 4.9.3. Cambios en los procedimientos de solicitud de revocación. Se describe el procedimiento de solicitud de revocación realizada por la AR o por la AC. Nuevo procedimiento de notificación de hechos que pueden indicar la necesidad de revocación de un certificado. 4.9.4. Se explican ejemplos de casos específicos que requieran una fecha de revocación futura. 4.9.5, 4.9.10. Se cambia la máxima la máxima latencia del servicio OCSP de las AC online a 10 minutos. 4.9.7. Actualización de AC. 4.9.11. Se describen los comunicados de revocación, suspensión y reactivación enviados al Titular del certificado de entidad final y los comunicados de revocación enviados al Suscriptor de certificados de AC Subordinada y TSU. 4.9.15. Se corrige el procedimiento de solicitud de suspensión. 4.10.2. Se describen los servicios de comprobación del estado de los certificados en caso de terminación de una AC bajo esta DPC y en

		caso de cese de actividad de Camerfirma como PSC. 5.2.1. Alineamiento con los roles de confianza en los estándares ETSI EN 319 401 y ETSI EN 319 411-1. 5.2.3, 5.2.4. Revisión. 5.4.3, 5.5.1, 5.5.2. Revisión. 5.6. Revisión y actualización. Se incluye la notificación de los nuevos certificados de AC y la terminación de la AC. 5.7.3. Revisión y actualización. Se incluye la terminación de la AC con la clave comprometida, la forma en que se sigue proporcionando el estado de revocación de los certificados emitidos por la AC con la clave comprometida, la revocación de una AC Subordinada externa con clave comprometida y la sustitución de la AC con la clave comprometida. 5.8. Revisión y actualización. Se divide el contenido de la sección 5.8 en las secciones 5.8.1 Cese de actividad y 5.8.2 Terminación de una AC. Nueva sección 5.8.3 Terminación de una AR. 6.1 y sus secciones. Revisión y actualización. 6.1.1. Actualización de AC. 6.2 y sus secciones. Revisión y actualización. 6.3.2. Revisión y actualización. Se indica el periodo de validez de los certificados bajo estas DPC y PC. 6.6. Revisión. 7 y sus secciones. Revisión y actualización. 7.2.2. Se incluyen las extensiones de CRL y de entrada de CRL. 7.3.2. Se incluyen las extensiones OCSP. 8 y sus secciones. Revisión y actualización. 8, 8.1, 8.2. Se añaden las auditorías ENS (Esquema Nacional de Seguridad). 9.1.3, 9.3.3.1. Revisión y actualización. Eliminación de sitios web. 9.5. Revisión. 9.6 y sus secciones. Revisión y actualización. 9.7. Revisión. 9.12.1, 9.12.2, 9.12.3, 9.16.1. Revisión. Otros cambios y correcciones menores.

26/02/2024	V1.5.0	El documento cambia su nombre de "Declaración de Prácticas de Certificación y Políticas de Certificación CAMERFIRMA 2008-2016" a "Declaración de Prácticas de Certificación y Políticas de Certificación CAMERFIRMA". Este documento da continuidad al documento "Declaración de Prácticas de Certificación y Políticas de Certificación CAMERFIRMA 2008-2016 Versión 1.4.0", incorporando el contenido actualizado del documento "Declaración de Prácticas de Certificación y Políticas de Certificación CAMERFIRMA 2021 Versión 1.1.0". Estos documentos, así como las versiones anteriores de los mismos pueden ser consultadas en: https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/practicas-de-certificacion-ac-camerfirma-cps-dpc-versiones-anteriores/ Se elimina el contenido correspondiente a la DPC de Camerfirma Perú porque sus AC se rigen ahora por su propia DPC. Esta versión especifica la DPC y las PC para la emisión de certificados por las AC activas de Camerfirma bajo las jerarquías de Camerfirma de 2008, 2016, 2021 y 2024 (Chambers of Commerce Root – 2008, CHAMBERS OF COMMERCE ROOT – 2016, GLOBAL CHAMBERSIGN ROOT – 2016, CAMERFIRMA ROOT 2021, INFOCERT-CAMERFIRMA ROOT 2024). Se actualiza la localización del documento en la portada. Se eliminan las siguientes AC terminadas y, en su caso, sus PC: - Jerarquía CHAMBERS OF COMMERCE ROOT – 2016: IVSIGN CA. - Jerarquía Chambers of Commerce – 2008: Camerfirma TSA – 2013. - Jerarquía Global Chambersign Root – 2008 (jerarquía de Camerfirma de 2008, sin AC activas): InfoCert Organization Validation CA 3, InfoCert Organization Validation 2019 CA 3, GLOBAL CORPORATE SERVER, AC Camerfirma Portugal – 2015, Global Chambersign Root – 2008. Se eliminan las siguientes PC terminadas (sin certificados activos) de AC activas: - Camerfirma TSA II – 2014: 1.3.6.1.4.1.17326.10.13.1.2 Se cambian las siguientes PC en AC activas: - AC CAMERFIRMA FOR LEGAL PERSONS – 2016: 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1. Se elimina QSCD

		Tarjeta/Token (sin certificados activos). Se añaden las siguientes nuevas AC: - INFOCERT-CAMERFIRMA CERTIFICATES 2024. - INFOCERT-CAMERFIRMA TIMESTAMP 2024 1.1. Revisión. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. Actualización de jerarquías y versiones de estándares ETSI. Se añaden los tipos de dispositivos QSCD y No QSCD en los que se generan las claves de los certificados emitidos por las AC bajo la DPC en este documento (se eliminan en la sección 1.3.1.1). 1.2. Eliminación de DPC de Camerfirma Perú. Actualización de jerarquías, PC y localización del documento. Se añaden las PC Certificado No Cualificado OCSP. 1.3.1. Actualización de domicilio social, teléfono y email de Camerfirma. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. Incorporación de la jerarquía CAMERFIRMA ROOT 2021. 1.3.1.1. Eliminación de los tipos de dispositivos QSCD y No QSCD en los que se generan las claves de los certificados emitidos por las AC bajo la DPC en este documento (se añaden en la sección 1.1). Actualización de AC y PC. Se añaden las PC Certificado No Cualificado OCSP. 1.3.1.1.3 y sus secciones. Actualización de AC, PC y FIPS. 1.3.1.1.6 y sus secciones. Eliminación por actualización de AC y PC. 1.3.1.2. Actualización de AC. Eliminación de contenido correspondiente a las DPC y PC de Camerfirma Perú. 1.3.1.2.2.1 y sus secciones. Eliminación por ser contenido correspondiente a la DPC y/o las PC de Camerfirma Perú. 1.3.1.2.3, 1.3.1.2.4. Eliminación por actualización de AC. Nueva sección 1.3.1.3, con sus secciones. Incorporación de la jerarquía CAMERFIRMA ROOT 2021. Nueva sección 1.3.1.4 con sus secciones. Incorporación de la jerarquía INFOCERT-CAMERFIRMA ROOT 2024 1.3.1.5. Revisión. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. Se añaden la generación y el almacenamiento de las claves de los certificados OCSP en un HSM FIPS 140-2 nivel 3 o CC EAL 4 o superior. 1.3.2. Eliminación de contenido correspondiente a la DPC de

		Camerfirma Perú. Se añaden las PC Certificado No Cualificado OCSP. 1.3.3.1, 1.3.3.2. Revisión. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 1.3.3.3, 1.3.3.4. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 1.3.3.5. Se añade el atributo *organizationIdenfier* del campo *subject* como dato de la Entidad identificada en un certificado. 1.3.5.1. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 1.4.2. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 1.5.2. Actualización de dirección, teléfono y email. 1.5.4. Actualización de la localización del documento. 1.6.1. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. Se añaden definiciones de entidad final, certificado de entidad final y certificado de AC. 1.6.2. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 2.2.1. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 2.2.4, 2.3. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 3.1.1. Actualización de la localización de las fichas de los perfiles de certificados bajo estas DPC y PC. 3.2.2.1. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 3.2.3. Revisión. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 3.3. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 3.3.1. Revisión. 3.4. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 4.1.2.3. Actualización de FIPS. 4.5.1. Actualización de AC y PC. Se añaden las PC Certificado No Cualificado OCSP.

		4.7.1. Revisión. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 4.7.2. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 4.7.3. Revisión. 4.9.1. Revisión y actualización. Se eliminan las causas de revocación alineadas con *Mozilla Root Store Policy*. 4.9.2. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 4.9.3. Revisión. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 4.9.4. Revisión. 4.9.5. Revisión. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 4.9.7, 4.9.8, 4.9.10. Revisión. Actualización de AC. 4.9.13. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 4.9.14. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 4.10.1, 4.10.2. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 5.5.1. Revisión. 5.7.3, 5.8.2. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 6.1.1. Actualización de AC. 6.1.5. Revisión. 6.1.6. Revisión. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 6.2.1.2. Actualización de FIPS. 6.3.2. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 7.1.3. Revisión. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 7.2.2. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021.

		8, 8.1, 8.2, 8.4. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 9.1.1. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 9.1.4. Actualización de la localización de estas DPC y PC. 9.1.5. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. 9.3.3.1. Actualización por incorporación de la jerarquía CAMERFIRMA ROOT 2021. 9.6.1.1, 9.6.2, 9.8, 9.12.2.2. Eliminación de contenido correspondiente a la DPC de Camerfirma Perú. Otros cambios y correcciones menores.
21/10/2024	1.5.1	9.6 La sección de obligaciones referencia a los términos y condiciones publicados en la página web. Otros cambios y correcciones menores.
26/05/2025	2.0	Simplificación de la DPC, elevándola a un documento general. Se eliminan las particularidades de cada tipo de certificado, que recogen en su propio documento de Política de Certificado (PC) Adaptación a la normativa siguiente: • Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014. • Directiva (UE) 2022/2555 (Directiva NIS 2) y su Reglamento de Ejecución de 17/10/2024. • ETSI EN 319401 V3.1.1 (2024-06) Limitación de renovación de certificados a 4 años en lugar de 5.