Tinexta Infocert

POLÍTICA DE CERTIFICACIÓN

PARA CERTIFICADOS PERSONALES

(FOR NATURAL PERSON)

CAMERFIRMA

Versión 1.0

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-2025-18-11

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2025.05.29 15:42:24 +02'00'

INDICE

1 INTRODUCCIÓN

1.1 VISIÓN GENERAL

La Política de Certificación (en adelante PC) es un documento que establece los requisitos, normas y procedimientos que rigen la emisión, uso, gestión y revocación de los certificados electrónicos. Su objetivo es garantizar la confianza y seguridad en la identidad digital de los titulares y en las transacciones que realizan con su certificado.

Por lo tanto, la presente PC establece los requisitos, normas y procedimientos aplicables a la emisión, uso, gestión y revocación de certificados electrónicos personales emitidos por Camerfirma.

En la Declaración de Prácticas de Certificación de Camerfirma (en adelante CPS) se recogen los conceptos básicos sobre certificados electrónicos, firma electrónica, Infraestructura de Clave Pública, etc… por lo que se recomienda que se consulte dicha CPS en caso de no tener conocimiento de dichos conceptos.

Este documento está estructurado de acuerdo con el estándar IETF RFC 3647.

Bajo esta PC, Camerfirma emite los siguientes tipos de certificados:

- **Certificado Cualificado de Ciudadano**:
  Este certificado cualificado identifica a una persona física (Titular/Firmante) únicamente para actuar en su propio nombre.

  Camerfirma emite estos certificados cualificados en dispositivos seguros de creación de firma - QSCD (tarjeta, token criptográfico o en nube) bajo el OID 0.4.0.194112.1.2 según ETSI EN 319 411-2 - QCP-n-qscd, y en dispositivos No QSCD bajo el OID 0.4.0.194112.1.0 según ETSI EN 319 411-2 - QCP-n

- **Certificado Cualificado Corporativo / de Autónomo / de Autónomo Colegiado**

  Certificado Cualificado Corporativo
  Este certificado cualificado identifica a una persona física (Titular/Firmante) y determina, como atributos específicos, su relación de vinculación (laboral, mercantil, colegial, etc.) con una Entidad.

  Certificado Cualificado de Autónomo
  Este certificado cualificado identifica a una persona física (Titular/Firmante) y determina, como atributos específicos, su condición de trabajador autónomo, su actividad económica y, si procede, el nombre comercial registrado bajo el cual el autónomo ejerce su profesión.

  Certificado Cualificado de Autónomo Colegiado
  Este certificado cualificado identifica a una persona física (Titular/Firmante) y determina, como atributos específicos, su condición de trabajador autónomo, su actividad económica, su

condición de profesional colegiado, y si procede, el nombre comercial registrado bajo el cual el autónomo ejerce su profesión.

Camerfirma emite estos certificados cualificados en dispositivos QSCD (tarjeta, token criptográfico o en nube) bajo el OID 0.4.0.194112.1.2 según ETSI EN 319 411-2 - QCP-n-qscd, y en dispositivos No QSCD) bajo el OID 0.4.0.194112.1.0 según ETSI EN 319 411-2 - QCP-n

- **Certificado de Representante Legal de Entidad con/sin Personalidad Jurídica**

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

Está dirigido a representantes legales de Entidades Con Personalidad Jurídica (Administrador Único, Administrador Solidario, Consejero-Delegado, etc.), a representantes legales de Entidades Sin Personalidad Jurídica (Administrador Único, Administrador Solidario, Director/Gerente, Presidente de la Comunidad de Propietarios, etc.), y a apoderados con facultades muy amplias de representación de Entidades Con o Sin Personalidad Jurídica (similares a las de un representante legal) que les permitan actuar tanto en el ámbito de las relaciones y trámites de la Entidad con las Administraciones Publicas (usos de autenticación y firma) como en el ámbito de la contratación de bienes o servicios relativos al funcionamiento ordinario de la Entidad (usos de firma).

Los representantes legales mancomunados que quieran solicitar este certificado deberán ostentar la facultad solidaria o específica general para actuar ante las Administraciones Públicas, en representación de la Entidad Con o Sin Personalidad Jurídica.

En todo caso, el Titular del certificado es responsable de utilizarlo de acuerdo con sus poderes y la Parte que Confía es responsable de verificar su contenido y alcance.

Los certificados emitidos bajo estas PC son conformes a la normativa nacional de los perfiles de certificados de persona física representante de persona jurídica y de persona física representante de entidad sin personalidad jurídica establecidos en el apartado 14.1 del documento “Perfiles de certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas, cuyo OID es 2.16.724.1.3.5.8 para representante de persona jurídica y OID 2.16.724.1.3.5.9 para representante de entidad sin personalidad jurídica.

Camerfirma emite estos certificados cualificados en dispositivos QSCD (tarjeta, token criptográfico o en nube) bajo el OID 0.4.0.194112.1.2 según ETSI EN 319 411-2 - QCP-n-qscd, y en dispositivos No QSCD bajo el OID 0.4.0.194112.1.0 según ETSI EN 319 411-2 - QCP-n.

- **Certificado de Representante Voluntario de Entidad con/sin Personalidad Jurídica ante las AAPP**

  Este certificado cualificado identifica a una persona física (Titular/Firmante) y determina, como atributos específicos, su capacidad para representar a una Entidad Con o Sin Personalidad Jurídica en el ámbito de sus relaciones y trámites con las Administraciones Públicas (usos de autenticación y firma).

  Está dirigido a apoderados con poder general o poder específico que incluya facultades que les permitan realizar, en nombre de la Entidad Con o Sin Personalidad Jurídica, actuaciones y trámites ante las Administraciones Públicas que requieran el uso de la firma electrónica o del certificado electrónico.

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

  En todo caso, el Titular del certificado es responsable de utilizarlo de acuerdo con sus poderes y la Parte que Confía es responsable de verificar su contenido y alcance.

  Los certificados emitidos bajo estas PC son conformes a la normativa nacional de los perfiles de certificados de persona física representante de persona jurídica y de persona física representante de entidad sin personalidad jurídica establecidos en el apartado 14.1 del documento “Perfiles de certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas, , cuyo OID es 2.16.724.1.3.5.8 para representante de persona jurídica y OID 2.16.724.1.3.5.9 para representante de entidad sin personalidad jurídica.

  Camerfirma emite estos certificados cualificados en dispositivos QSCD (tarjeta, token criptográfico o en nube) bajo el OID 0.4.0.194112.1.2 según ETSI EN 319 411-2 - QCP-n-qscd, y en dispositivos No QSCD) bajo el OID 0.4.0.194112.1.0 según ETSI EN 319 411-2 - QCP-n.

- **Certificado de apoderado de Entidad con/sin Personalidad Jurídica**

  Este certificado cualificado identifica a una persona física (Titular/Firmante) y determina, como atributos específicos, su capacidad para actuar en nombre de una Entidad Con o Sin Personalidad jurídica solo para determinadas facultades enmarcadas en su función o departamento en la Entidad (usos de firma de documentos privados del tráfico mercantil ordinario de la Entidad).

  Este certificado no es válido para usos de autenticación o firma en nombre de la Entidad Con o Sin Personalidad Jurídica en plataformas de la Administración Pública, por la limitación

implícita de los poderes cuyo alcance exacto no puede conocer la Parte que Confía.
Los apoderados mancomunados que quieran solicitar este certificado deberán ostentar poderes que incluyan las correspondientes facultades solidarias enmarcadas en su función o departamento en la Entidad. Alternativamente, pueden aportar un poder específico o un documento fehaciente firmado por todos los apoderados conjuntamente a favor de uno de ellos.

En todo caso, el Titular/Firmante del certificado es responsable de utilizarlo de acuerdo con sus facultades y la Parte que Confía es responsable de verificar su contenido y alcance.

Camerfirma emite estos certificados cualificados en dispositivos QSCD (tarjeta, token criptográfico o en nube) bajo el OID 0.4.0.194112.1.2 según ETSI EN 319 411-2 - QCP-n-qscd, y en dispositivos No QSCD) bajo el OID 0.4.0.194112.1.0 según ETSI EN 319 411-2 - QCP-n.

- **Certificados de Empleado Público Con/Sin Seudónimo**

Estos certificados identifican a una persona física (Titular/Firmante) como empleado público.

Los certificados cualificados emitidos bajo esta PC pueden ser usados por los sistemas de firma electrónica del personal al servicio de las Administraciones Públicas, conforme a lo establecido en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados emitidos bajo estas PC son conformes a la normativa nacional de los perfiles de certificados de empleado público y de empleado público con seudónimo establecidos en los apartados 10 y 11 del documento “Perfiles de certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas con los siguientes OID de Política según normativa nacional:

- en sus niveles alto:
  - certificado de empleado: OID 2.16.724.1.3.5.7.1
  - certificado de empleado con seudónimo: OID 2.16.724.1.3.5.4.1
- en su nivel medio/sustancial:
  - certificado de empleado: OID 2.16.724.1.3.5.7.2
  - certificado de empleado con seudónimo: OID 2.16.724.1.3.5.4.2

Camerfirma emite estos certificados cualificados de firma en dispositivos QSCD (tarjeta, token criptográfico o en nube) bajo el OID 0.4.0.194112.1.2 según ETSI EN 319 411-2 -QCP-n-qscd, y en dispositivos No QSCD bajo el OID 0.4.0.194112.1.0 según ETSI EN 319 411-2-QCP-n.

Camerfirma emite certificados no cualificados de empleado público con y sin seudónimo de autenticación y de cifrado, siempre en nube. Estos certificados son no cualificados porque no son susceptibles de cualificar. Los OIDs de Política según la normativa nacional para estos certificados son los mismos que los relacionados en el párrafo anterior. El OID del certificado no cualificado de autenticación es 0.4.0.2042.1.2 según ETSI EN 319 411-1 - NCP+.

En la presente Política de Certificación se exponen las condiciones particulares referentes a los

tipos de certificados que integran esta PC.

1.2 IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

Nombre:	Política de Certificación para certificados personales de CAMERFIRMA
Descripción:	Políticas de Certificación para certificados personales, que generan firma electrónica avanzada o cualificada
Versión:	Ver página inicial
OID:	• **Certificado Cualificado de Ciudadano** Jerarquía CHAMBERS OF COMMERCE ROOT – 2016 ○ 1.3.6.1.4.1.17326.10.16.1.1.1: QSCD Tarjeta/Token ○ 1.3.6.1.4.1.17326.10.16.1.1.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube ○ 1.3.6.1.4.1.17326.10.16.1.1.2: No QSCD Jerarquía CAMERFIRMA ROOT 2021 ○ 1.3.6.1.4.1.17326.10.21.1.1.1: QSCD Tarjeta/Token ○ 1.3.6.1.4.1.17326.10.21.1.1.3: QSCD Nube Jerarquía INFOCERT-CAMERFIRMA ROOT 2024 ○ 1.3.6.1.4.1.17326.10.21.1.1.2: No QSCD • **Certificado Cualificado Corporativo / de Autónomo / de Autónomo Colegiado** Jerarquía CHAMBERS OF COMMERCE ROOT – 2016 ○ 1.3.6.1.4.1.17326.10.16.1.2.1: QSCD Tarjeta/Token ○ 1.3.6.1.4.1.17326.10.16.1.2.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube ○ 1.3.6.1.4.1.17326.10.16.1.2.2 - No QSCD Jerarquía CAMERFIRMA ROOT 2021 ○ 1.3.6.1.4.1.17326.10.21.1.2.1: QSCD Tarjeta/Token ○ 1.3.6.1.4.1.17326.10.21.1.2.3: QSCD Nube • **Certificados Cualificados de Representante** Jerarquía CHAMBERS OF COMMERCE ROOT – 2016 ○ Representante Legal de Entidad Con/Sin Personalidad Jurídica ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.1: QSCD Tarjeta/Token ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube ▪ 1.3.6.1.4.1.17326.10.16.1.3.1.2: No QSCD ○ Representante Voluntario de Entidad Con/Sin Personalidad Jurídica ante las AAPP ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.1: QSCD Tarjeta/Token ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube ▪ 1.3.6.1.4.1.17326.10.16.1.3.2.2: No QSCD ○ Apoderado de Entidad Con/Sin Personalidad Jurídica ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.1: QSCD Tarjeta/Token ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube ▪ 1.3.6.1.4.1.17326.10.16.1.3.3.2: No QSCD Jerarquía CAMERFIRMA ROOT 2021 ○ Representante Legal de Entidad Con Personalidad Jurídica

- 1.3.6.1.4.1.17326.10.21.1.3.1: QSCD Tarjeta/Token
- 1.3.6.1.4.1.17326.10.21.1.3.3: QSCD Nube

- Representante Legal de Entidad Sin Personalidad Jurídica
  - 1.3.6.1.4.1.17326.10.21.1.4.1: QSCD Tarjeta/Token
  - 1.3.6.1.4.1.17326.10.21.1.4.3: QSCD Nube
- Representante Voluntario de Entidad Con Personalidad Jurídica ante las AAPP
  - 1.3.6.1.4.1.17326.10.21.1.5.1: QSCD Tarjeta/Token
  - 1.3.6.1.4.1.17326.10.21.1.5.3: QSCD Nube
- Representante Voluntario de Entidad Sin Personalidad Jurídica ante las AAPP
  - 1.3.6.1.4.1.17326.10.21.1.6.1: QSCD Tarjeta/Token
  - 1.3.6.1.4.1.17326.10.21.1.6.3: QSCD Nube
- Apoderado de Entidad Con Personalidad Jurídica
  - 1.3.6.1.4.1.17326.10.21.1.7.1: QSCD Tarjeta/Token
  - 1.3.6.1.4.1.17326.10.21.1.7.3: QSCD Nube
- Apoderado de Entidad Sin Personalidad Jurídica
  - 1.3.6.1.4.1.17326.10.21.1.8.1: QSCD Tarjeta/Token
  - 1.3.6.1.4.1.17326.10.21.1.8.3: QSCD Nube

- **Certificados de Empleado Público Con/Sin Seudónimo**
  Jerarquía CHAMBERS OF COMMERCE ROOT – 2016
  - Certificado Cualificado de Firma - Nivel Alto
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1: QSCD Tarjeta/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.1, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube
  - Certificado No Cualificado de Autenticación - Nivel Alto
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2: Tarjeta/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.2, 1.3.6.1.4.1.17326.99.18.1: Nube
  - Certificado No Cualificado de Cifrado - Nivel Alto
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3: Tarjeta/Token
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.3, 1.3.6.1.4.1.17326.99.18.1: Nube
  - Certificado Cualificado - Nivel Medio
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4: QSCD Tarjeta/Token / No QSCD
    - 1.3.6.1.4.1.17326.10.16.1.5.1.3.4.4, 1.3.6.1.4.1.17326.99.18.1: QSCD Nube
  -

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

Anteriormente, esta Política estaba contenida en la DPC general. Para una mejor comprensión y gestión de los documentos, se separa esta Política de Certificación para Certificados Personales y se emite una nueva versión de la DPC, complementaria a esta PC.

1.3 PARTICIPANTES EN LA PKI

1.3.1 AUTORIDADES DE CERTIFICACIÓN (AC)

Bajo esta PC, Camerfirma gestiona las siguientes jerarquías de AC:

- CHAMBERS OF COMMERCE ROOT:
    - AC CAMERFIRMA FOR NATURAL PERSONS – 2016
- GLOBAL CHAMBERSIGN ROOT
- CAMERFIRMA ROOT 2021
    - AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021
- INFOCERT-CAMERFIRMA ROOT 2024
    - INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES – 2024

1.3.1.1 CERTIFICADOS DE PRUEBAS

Según lo dispuesto en la CPS.

1.3.1.2 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 esta PC.

1.3.2 AUTORIDADES DE REGISTRO (AR)

Bajo esta PC 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 PC, 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 identificar al Solicitante mediante personación 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.

1.3.3 SUSCRIPTORES

1.3.3.1 SUSCRIPTOR

Bajo esta PC, el Suscriptor de un certificado puede ser:

- Para los certificados emitidos a personas físicas sin atributos de vinculación a una Entidad:
  - La persona física Titular.
  - Una persona jurídica o una entidad sin personalidad jurídica a la que está vinculada la persona física Titular.
- Para los certificados emitidos a personas físicas con atributos de vinculación a una Entidad (persona jurídica o entidad sin personalidad jurídica):
  - La persona física Titular.
  - La Entidad (persona jurídica o entidad sin personalidad jurídica) identificada en el certificado a la que está vinculada la persona física Titular.
  - Una persona jurídica o una entidad sin personalidad jurídica a la que está vinculada la persona física Titular (distinta a la Entidad identificada en el certificado).

Para evitar un conflicto de intereses, el Suscriptor de un certificado y Camerfirma, como PSC emisor del certificado (AC bajo esta PC), o las AR bajo esta PC deben ser entidades independientes. Las únicas excepciones son:

- Una tercera organización que actúe como AR bajo esta PC y como Suscriptor de los certificados emitidos para los Titulares vinculados a ella.
- Certificados que Camerfirma emite para sí misma (como Entidad persona jurídica) o para personas físicas que forman parte de ella (como Titular).

Para ambas excepciones, la solicitud, la validación y la tramitación de los certificados deben realizarse según los procesos definidos por Camerfirma para los respectivos tipos de certificados.

1.3.3.2 TITULAR Y FIRMANTE

Bajo esta PC, el Titular de un certificado puede ser:

- Para los certificados emitidos a personas físicas sin atributos de vinculación a una Entidad:
    - La persona física a la que se emite el certificado. El Suscriptor puede ser:
        - El Titular (la persona física identificada en el certificado).
        - Una persona jurídica o una entidad sin personalidad jurídica a la que está vinculada el Titular.
- Para los certificados emitidos a personas físicas con atributos de vinculación a una Entidad (persona jurídica o entidad sin personalidad jurídica):
    - La persona física a la que se emite el certificado. El Suscriptor puede ser:
        - El Titular (la persona física identificada en el certificado).
        - La Entidad identificada en el certificado a la que está vinculado el Titular (la persona jurídica o la entidad sin personalidad jurídica identificada en el certificado).
        - Una persona jurídica o una entidad sin personalidad jurídica a la que está vinculada el Titular (distinta a la Entidad identificada en el certificado).

Bajo esta PC, y de acuerdo con el Reglamento eIDAS, el Firmante es la persona física identificada en un certificado de firma electrónica.

Bajo estas PC, el Firmante de un certificado pueden ser:

- Para los certificados emitidos a personas físicas, con o sin atributos de vinculación a una Entidad, cualificados, o no cualificados con uso permitido de firma:
    - El Firmante es la persona física Titular (la persona física identificada en el certificado).
- Para el resto de certificados emitidos a personas físicas (certificados no cualificados de autenticación o de cifrado, con atributos de vinculación a una Entidad, sin uso permitido de firma)
    - No hay Firmante.

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.

En esta PC, el término “Titular/Firmante” se refiere, de forma genérica, al Titular y/o Firmante de los certificados emitidos a personas físicas.

1.3.3.3 SOLICITANTE

Bajo estas PC, el Solicitante de un certificado será la persona física titular del mismo.

1.3.4 RESPONSABLE

Bajo esta PC, 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.

Bajo estas PC, el Responsable de un certificado puede ser el Solicitante, o una persona física autorizada por el Solicitante, sin perjuicio de las obligaciones del Firmante y, en su caso, del Titular.

1.3.5 PARTES QUE CONFÍAN

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

1.3.6 OTROS PARTICIPANTES

1.3.6.1 ORGANISMO DE SUPERVISIÓN

Según lo dispuesto en la CPS.

1.4 USOS DEL CERTIFICADO

1.4.1 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados emitidos bajo estas PC se usan para los siguientes propósitos:

- Autenticación del Titular.
- Firma electrónica cualificada o firma electrónica avanzada, dependiendo de si el certificado está emitido en dispositivos cualificados de creación firma electrónica o no.
- Cifrado asimétrico o mixto sin recuperación de clave.

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

Según lo dispuesto en la CPS.

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Según lo dispuesto en la CPS.

1.5.2 DATOS DE CONTACTO

Según lo dispuesto en la CPS.

1.5.3 PERSONA QUE DETERMINA LA IDONEIDAD DE DPC PARA LA POLÍTICA

Según lo dispuesto en la CPS.

1.5.4 PROCEDIMIENTOS DE GESTIÓN DEL DOCUMENTO

Según lo dispuesto en la CPS.

1.6 DEFINICIONES Y SIGLAS

Según lo dispuesto en la CPS

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 esta PC en el sitio web siguiente:

- 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 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.

2.2.2 TÉRMINOS Y CONDICIONES

Según lo dispuesto en la CPS

2.2.3 DIFUSIÓN DE LOS CERTIFICADOS

Según lo dispuesto en la CPS.

2.2.4 CRL Y OCSP

Según lo dispuesto en la CPS.

2.3 FRECUENCIA DE PUBLICACIÓN

Según lo dispuesto en la CPS.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Según lo dispuesto en la CPS.

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.

La estructura y el contenido del DN en el campo *Subject* y, en su caso, de los campos en la extensión *Subject Alternative Name* se describen en las fichas de los perfiles de certificados, incluyendo como mínimo:

- Para los certificados de entidad final emitidos a personas físicas sin atributos de vinculación a una Entidad:
    - Nombre y apellidos e identificador fiscal de la persona física Titular.
- Para los certificados de entidad final emitidos a personas físicas con atributos de vinculación a una Entidad (persona jurídica o entidad sin personalidad jurídica):
    - Nombre y apellidos e identificador fiscal de la persona física Titular.
    - Denominación social e identificador fiscal de la Entidad.

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

Las fichas de los perfiles de certificados bajo esta PC se pueden solicitar a través del servicio de soporte a cliente de Camerfirma en el sitio web https://www.camerfirma.com/contacto-soporte o en el teléfono +34 91 136 91 05.

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. Los campos del DN referidos a “nombre y apellidos” del titular deberá ser igual a los datos presentados mediante el documento de identidad fehaciente, y con el mismo formato.

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

Según lo dispuesto en la CPS.

3.1.5 UNICIDAD DE LOS NOMBRES

Según lo dispuesto en la CPS.

3.1.6 PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS DE NOMBRES

Según lo dispuesto en la CPS.

3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1 MÉTODOS DE PRUEBA DE LA POSESIÓN DE LA CLAVE PRIVADA

Antes de emitir un certificado, es obligatorio verificar la identidad del solicitante mediante la presentación de un documento de identidad válido. Los documentos aceptados varían según la nacionalidad y la situación del solicitante:

- 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.

La autenticación puede realizarse mediante diferentes métodos conforme al Reglamento eIDAS y la normativa nacional:

- Personación física ante la Autoridad de Certificación (AC), Autoridad de Registro (AR) o en un Punto de Verificación Presencial (PVP). También se acepta la comparecencia ante notario con firma legitimada.
- Identificación electrónica a distancia, mediante sistemas de identificación notificados por los Estados miembros en virtud del artículo 9.1 del Reglamento eIDAS, siempre que cumplan un nivel de seguridad "alto". En España, se ha notificado el DNI electrónico.
- Uso de firma electrónica cualificada con u certificado emitido por una AC de Camerfirma o de otro PCSC, siempre que contengan los datos de identidad del solicitante.
- Métodos de identificación remota por vídeo, conforme a la Orden ETD/465/2021,

incluyendo procesos asistidos (con operador) y desasistidos (revisión posterior).

En estos procesos de identificación remota por video, Camerfirma podrá verificar los datos del solicitante con fuentes oficiales, almacenar registros de audio/vídeo y aplicar restricciones en la aceptación de documentos de identidad.

Lo dispuesto en esta sección sobre la obligación de comprobación de la identidad del Solicitante de un certificado cualificado 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 la identificación presencial y el período de tiempo transcurrido desde la identificación fuese menor de cinco años.

Para certificados no cualificados, además de los métodos anteriores, pueden aceptarse identificaciones mediante firmas electrónicas avanzadas o métodos de identificación por vídeo no reconocidos a escala nacional.

3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN

Según lo dispuesto en la CPS

3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE

Según lo dispuesto en la CPS

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 persona física con al empresa y organismo a la que representa o a la que está adherido o registrado, a traves de la documentación siguiente:

Tipo de certificado	Documentación
Certificado Cualificado Corporativo	Normalmente, autorización firmada por un representante legal o apoderado general de la Entidad.
Certificado Cualificado de Autónomo Certificado Cualificado de Autónomo Colegiado	Documentación acreditativa de la condición de autónomo en régimen de actividad económica, y si es un profesional colegiado, de su colegiación en un Colegio profesional (colegiatura activa). De forma opcional, documentación acreditativa del nombre comercial registrado

	bajo el cual ejerce su actividad.
Certificado Cualificado de Representante Legal de Entidad Con/Sin Personalidad Jurídica Certificado Cualificado de Representante Voluntario de Entidad Con/Sin Personalidad Jurídica ante las AAPP Certificado Cualificado de Apoderado de Entidad Con/Sin Personalidad Jurídica	Documentación acreditativa de las facultades de representación de la Entidad, en función del tipo de representante y del tipo de Entidad.
Certificados de Empleado Público Con/Sin Seudónimo	Autorización firmada por una persona con facultades de representación de la Entidad donde se indique que es empleado público, o nombramiento en Boletín Oficial donde conste el DNI/NIE de esta persona.
Certificado No Cualificado de Personal AAPP	Autorización firmada por una persona con facultades de representación de la Entidad donde se indique que es empleado público, o nombramiento en Boletín Oficial donde conste el DNI/NIE de esta persona.

3.2.5.2 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

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE UNA SOLICITUD DE REVOCACIÓN

Según lo dispuesto en la CPS

4 REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

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

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.

4.2 PROCESAMIENTO DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Según lo dispuesto en la CPS

4.2.2 APROBACIÓN O RECHAZO DE LA SOLICITUD

Según lo dispuesto en la CPS

4.2.3 PLAZO PARA RESOLVER LA SOLICITUD

Según lo dispuesto en la CPS

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE LA AC DURANTE EL PROCESO DE EMISIÓN

Según lo dispuesto en la CPS.

4.3.2 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO AL SUSCRIPTOR

Para los certificados emitidos bajo esta CP, se notfica mediante un correo electrónico al Responsable indicando la aprobación o denegación de la solicitud.

4.4 ACEPTACIÓN DE CERTIFICADOS

4.4.1 CONDUCTA QUE CONSTITUYE LA ACEPTACIÓN DEL CERTIFICADO

Según lo dispuesto en la CPS

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA AC

Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

4.5 USO DEL PAR DE CLAVES Y LOS CERTIFICADOS

4.5.1 USO DEL CERTIFICADO Y LA CLAVE PRIVADA DEL SUSCRIPTOR

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

AC/PC	Key Usage	Extended Key Usage	Basic Constraints
CHAMBERS OF COMMERCE ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA FOR NATURAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical, CA:true, pathLen:2
Certificado Cualificado de Ciudadano - QSCD Tarjeta/Token, QSCD Nube, No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado Corporativo / de Autónomo / de Autónomo Colegiado - QSCD Tarjeta/Token, QSCD Nube, No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado de Representante Legal de Entidad Con/Sin Personalidad Jurídica - QSCD Tarjeta/Token, QSCD Nube, No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false

Certificado Cualificado de Representante Voluntario de Entidad Con/Sin Personalidad Jurídica ante las AAPP - QSCD Tarjeta/Token, QSCD Nube, No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado de Apoderado de Entidad Con/Sin Personalidad Jurídica - QSCD Tarjeta/Token, QSCD Nube, No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado de Firma de Empleado Público Con/Sin Seudónimo - Nivel Alto - QSCD Tarjeta/Token, QSCD Nube	critical, contentCommitment	-	critical, CA:false
Certificado No Cualificado de Autenticación de Empleado Público Con/Sin Seudónimo - Nivel Alto - Tarjeta/Token, Nube	critical, digitalSignature	emailProtection clientAuth	critical, CA:false
Certificado No Cualificado de Cifrado de Empleado Público - Nivel Alto - Tarjeta/Token, Nube	critical, keyEncipherment, dataEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado de Empleado Público Con/Sin Seudónimo - Nivel Medio - QSCD Tarjeta/Token / No QSCD, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
CAMERFIRMA ROOT 2021	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0
Certificado Cualificado de Ciudadano – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Certificado Cualificado Corporativo – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false

Certificado Cualificado de Representante Legal de Entidad Con Personalidad Jurídica – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Certificado Cualificado de Representante Legal de Entidad Sin Personalidad Jurídica – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Certificado Cualificado de Representante Voluntario de Entidad Con Personalidad Jurídica ante las AAPP – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Certificado Cualificado de Representante Voluntario de Entidad Sin Personalidad Jurídica ante las AAPP – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Certificado Cualificado de Apoderado de Entidad Con Personalidad Jurídica – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
Certificado Cualificado de Apoderado de Entidad Sin Personalidad Jurídica – QSCD Tarjeta/Token, QSCD Nube	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection, clientAuth	critical, CA:false
INFOCERT-CAMERFIRMA CERTIFICATES 2024	critical, cRLSign, keyCertSign	-	critical, CA:true
INFOCERT-CAMERFIRMA QUALIFIED CERTIFICATES - 2024	critical, cRLSign, keyCertSign	Adobe Trust, clientAuth	critical, CA:true, pathLen:0
Certificado Cualificado de Ciudadano - No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false

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

Para los certificados de firma remota, el Titular/Firmante debe conservar las herramientas y/o dispositivos de autenticación de la firma remota de forma segura. Asimismo, debe mantener el PIN de activación de la clave privada del certificado de firma remota bajo su control exclusivo y de forma separada a las contraseñas de autenticación o dispositivos de autenticación. Finalmente debe asegurarse de mantener la privacidad y preservación del PIN de revocación del certificado. El Titular/Firmante no debe crear firmas digitales con claves privadas de certificados suspendidos o revocados ni utilizar certificados de AC revocados.

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

Según lo dispuesto en la CPS

4.5.3 CIRCUNSTANCIAS PARA LA RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

No estipulado.

4.5.4 QUIÉN PUEDE SOLICITAR LA RENOVACIÓN SIN CAMBIO DE CLAVES

No estipulado.

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

No estipulado.

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

No estipulado.

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

No estipulado.

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

No estipulado.

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

No estipulado.

4.6 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Según lo dispuesto en la CPS.

4.6.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Para los certificados emitidos bajo esta CP, un certificado puede ser renovado con cambio de claves antes de su fecha de caducidad.

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

- 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, han trascurrido más de 4 años desde la última identificación presencial del Solicitante.

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

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

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

Se Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

4.7 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.

4.8 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

Según lo dispuesto en la CPS

4.8.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Según lo dispuesto en la CPS

4.8.2 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

Según lo dispuesto en la CPS

4.8.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

Según lo dispuesto en la CPS.

4.8.4 PERIODO DE GRACIA DE LA SOLICITUD DE REVOCACIÓN

Según lo dispuesto en la CPS

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

Según lo dispuesto en la CPS

4.8.6 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

Según lo dispuesto en la CPS

4.8.7 FRECUENCIA DE EMISIÓN DE CRL

Según lo dispuesto en la CPS

4.8.8 MÁXIMA LATENCIA PARA CRL

Según lo dispuesto en la CPS.

4.8.9 DISPONIBILIDAD DE COMPROBACIÓN EN LÍNEA DE LA REVOCACIÓN

Según lo dispuesto en la CPS

4.8.10 REQUISITOS DE LA COMPROBACIÓN EN LÍNEA DE LA REVOCACIÓN

Según lo dispuesto en la CPS

4.8.11 OTRAS FORMAS DE ANUNCIOS DE REVOCACIÓN DISPONIBLES

Según lo dispuesto en la CPS

4.8.12 REQUISITOS ESPECIALES EN RELACIÓN CON EL COMPROMISO DE CLAVES PRIVADAS

Según lo dispuesto en la CPS

4.8.13 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

Según lo dispuesto en la CPS

4.8.14 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Según lo dispuesto en la CPS

4.8.15 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

Según lo dispuesto en la CPS

4.8.16 LÍMITES DEL PERIODO DE SUSPENSIÓN

Según lo dispuesto en la CPS

4.9 SERVICIOS DE COMPROBACIÓN DEL ESTADO DE LOS CERTIFICADOS

4.9.1 CARACTERÍSTICAS OPERACIONALES

Según lo dispuesto en la CPS.

4.9.2 DISPONIBILIDAD DEL SERVICIO

Según lo dispuesto en la CPS.

4.10 FINALIZACIÓN DE LA SUSCRIPCIÓN

Según lo dispuesto en la CPS.

4.11 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.11.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

Según lo dispuesto en la CPS.

4.11.2 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

Según lo dispuesto en la CPS.

5.1.1 UBICACIÓN Y CONSTRUCCIÓN

Según lo dispuesto en la CPS.

5.1.2 ACCESO FÍSICO

Según lo dispuesto en la CPS.

5.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Según lo dispuesto en la CPS.

5.1.4 EXPOSICIÓN AL AGUA

Según lo dispuesto en la CPS.

5.1.5 PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

Según lo dispuesto en la CPS.

5.1.6 SISTEMA DE ALMACENAMIENTO

Según lo dispuesto en la CPS.

5.1.7 ELIMINACIÓN DE RESIDUOS

Según lo dispuesto en la CPS.

5.1.8 COPIA DE RESPALDO EXTERNA

Según lo dispuesto en la CPS.

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

Según lo dispuesto en la CPS.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Según lo dispuesto en la CPS.

5.2.3 IDENTIFICACIÓN Y AUTENTIFICACIÓN PARA CADA ROL

Según lo dispuesto en la CPS.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE TAREAS

Según lo dispuesto en la CPS.

5.3 CONTROLES DEL PERSONAL

5.3.1 CALIFICACIONES, EXPERIENCIA Y REQUISITOS DE AUTORIZACIÓN

Según lo dispuesto en la CPS.

5.3.2 PROCEDIMIENTOS DE COMPROBACIÓN DE ANTECEDENTES

Según lo dispuesto en la CPS.

5.3.3 REQUERIMIENTOS DE FORMACIÓN

Según lo dispuesto en la CPS.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE LA ACTUALIZACIÓN DE LA FORMACIÓN

Según lo dispuesto en la CPS.

5.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

No estipulado.

5.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Según lo dispuesto en la CPS.

5.3.7 REQUERIMIENTOS DE CONTRATACIÓN DE PERSONAL

Según lo dispuesto en la CPS.

5.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

Según lo dispuesto en la CPS.

5.4 PROCEDIMIENTOS DE REGISTRO DE EVENTOS

Según lo dispuesto en la CPS.

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Según lo dispuesto en la CPS.

5.4.2 PERIODOS DE RETENCIÓN PARA LOS REGISTROS DE AUDITORIA

Según lo dispuesto en la CPS.

5.4.3 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Según lo dispuesto en la CPS.

5.4.4 PROCEDIMIENTOS DE COPIA DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Según lo dispuesto en la CPS.

5.4.5 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA

Según lo dispuesto en la CPS.

5.4.6 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

Según lo dispuesto en la CPS.

Análisis de vulnerabilidades

Según lo dispuesto en la CPS.

5.5 ARCHIVO DE REGISTROS

5.5.1 TIPO DE ARCHIVOS REGISTRADOS

Según lo dispuesto en la CPS.

5.5.2 PERIODO DE RETENCIÓN PARA EL ARCHIVO

Según lo dispuesto en la CPS.

5.5.3 PROTECCIÓN DEL ARCHIVO

Según lo dispuesto en la CPS.

5.5.4 PROCEDIMIENTOS DE COPIA DE RESPALDO DEL ARCHIVO

Según lo dispuesto en la CPS.

5.5.5 REQUERIMIENTOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Según lo dispuesto en la CPS.

5.5.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORIA

No estipulado.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Según lo dispuesto en la CPS.

5.6 CAMBIO DE CLAVES

Según lo dispuesto en la CPS.

5.7 RECUPERACIÓN EN CASO DE COMPROMISO DE LA CLAVE O DESASTRE

Según lo dispuesto en la CPS.

5.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENCIAS Y COMPROMISOS

Según lo dispuesto en la CPS.

5.7.2 CORRUPCIÓN DE RECURSOS, APLICACIONES O DATOS

Según lo dispuesto en la CPS.

5.7.3 COMPROMISO DE LA CLAVE PRIVADA DE LA AC

Según lo dispuesto en la CPS.

5.7.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Según lo dispuesto en la CPS.

5.8 TERMINACIÓN DE UNA AC O UNA AR

5.8.1 CESE DE ACTIVIDAD

Según lo dispuesto en la CPS.

5.8.2 TERMINACIÓN DE UNA AC

Según lo dispuesto en la CPS.

5.8.3 TERMINACIÓN DE UNA AR

Según lo dispuesto en la CPS.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

Según lo dispuesto en la CPS.

6.1.2 ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Según lo dispuesto en la CPS.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS.

6.1.5 TAMAÑO DE LAS CLAVES

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS.

6.1.7 PROPÓSITOS DE USO DE CLAVES

Según lo dispuesto en la CPS.

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

6.2.1 CONTROLES Y ESTÁNDARES DE MÓDULOS CRIPTOGRÁFICOS

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS.

6.2.3 DEPÓSITO DE CLAVE PRIVADA

Según lo dispuesto en la CPS.

6.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

Según lo dispuesto en la CPS.

6.2.5 ARCHIVO DE LA CLAVE PRIVADA

Según lo dispuesto en la CPS.

6.2.6 INTRODUCCIÓN DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Según lo dispuesto en la CPS.

6.2.7 ALMACENAMIENTO DE CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Según lo dispuesto en la CPS.

6.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Según lo dispuesto en la CPS.

6.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Según lo dispuesto en la CPS.

6.2.10 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

Según lo dispuesto en la CPS.

6.2.11 CALIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

Según lo dispuesto en la CPS.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Según lo dispuesto en la CPS.

6.3.2 PERIODO DE USO PARA LAS CLAVES PÚBLICAS Y PRIVADAS

Según lo dispuesto en la CPS.

6.4 DATOS DE ACTIVACIÓN DE LAS CLAVES PRIVADAS

6.4.1 GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Según lo dispuesto en la CPS.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Según lo dispuesto en la CPS.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No estipulado.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Según lo dispuesto en la CPS.

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD INFORMÁTICA ESPECÍFICOS

Según lo dispuesto en la CPS.

6.5.2 VALORACIÓN DE LA SEGURIDAD INFORMÁTICA

Según lo dispuesto en la CPS.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Según lo dispuesto en la CPS.

6.6.1 CONTROLES DE DESARROLLO DEL SISTEMA

Según lo dispuesto en la CPS.

6.6.2 CONTROLES DE GESTIÓN DE LA SEGURIDAD

Según lo dispuesto en la CPS.

6.6.3 GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO

Según lo dispuesto en la CPS.

6.6.4 EVALUACIÓN DE LA SEGURIDAD DEL CICLO DE VIDA

No estipulado.

6.7 CONTROLES DE SEGURIDAD DE LA RED

Según lo dispuesto en la CPS.

6.8 FUENTES DE TIEMPO

Según lo dispuesto en la CPS.

7 PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 PERFILES DE CERTIFICADOS

Según lo dispuesto en la CPS.

7.1.1 NÚMERO DE VERSIÓN

Todos los certificados son X.509 versión 3.

7.1.2 EXTENSIONES DEL CERTIFICADO

Según lo dispuesto en la CPS.

7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Según lo dispuesto en la CPS.

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 PC.

En general, los certificados de empleado 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.

7.1.5 RESTRICCIONES DE LOS NOMBRES

Según lo dispuesto en la CPS.

7.1.6 IDENTIFICADOR DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICACIÓN

Según lo dispuesto en la CPS.

7.1.7 USO DE LA EXTENSIÓN "POLICY CONSTRAINTS"

Según lo dispuesto en la CPS.

7.1.8 SINTAXIS Y SEMÁNTICA DE LOS CALIFICADORES DE POLÍTICA

Según lo dispuesto en la CPS.

7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA "CERTIFICATE POLICES"

Según lo dispuesto en la CPS.

7.2 PERFILES DE CRL

Según lo dispuesto en la CPS.

7.2.1 NÚMERO DE VERSIÓN

Según lo dispuesto en la CPS.

7.2.2 EXTENSIONES DE CRL Y DE ENTRADA DE CRL

Según lo dispuesto en la CPS.

7.3 PERFILES DE OCSP

Según lo dispuesto en la CPS.

7.3.1 NÚMERO DE VERSIÓN

Según lo dispuesto en la CPS.

7.3.2 EXTENSIONES OCSP

Según lo dispuesto en la CPS.

8 AUDITORÍAS DE CONFORMIDAD

Según lo dispuesto en la CPS.

8.1 FRECUENCIA DE LAS AUDITORÍAS

Según lo dispuesto en la CPS.

8.1.1 AUDITORÍAS DE AC SUBORDINADA EXTERNA O CERTIFICACIÓN CRUZADA.

No aplicable.

8.1.2 AUDITORIA EN LAS AR

Según lo dispuesto en la CPS.

8.1.3 AUDITORÍAS INTERNAS

Según lo dispuesto en la CPS.

8.2 IDENTIFICACIÓN Y CUALIFICACIONES DEL AUDITOR

Según lo dispuesto en la CPS.

8.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Según lo dispuesto en la CPS.

8.4 PUNTOS CUBIERTOS POR LA AUDITORIA

Según lo dispuesto en la CPS.

8.5 MEDIDAS TOMADAS COMO RESULTADO DE LAS DEFICIENCIAS

Según lo dispuesto en la CPS.

8.6 COMUNICACIÓN DE RESULTADOS

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS.

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

Según lo dispuesto en la CPS.

9.1.4 TARIFAS DE OTROS SERVICIOS

Según lo dispuesto en la CPS.

9.1.5 POLÍTICA DE REINTEGROS

Según lo dispuesto en la CPS.

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DEL SEGURO

Según lo dispuesto en la CPS.

9.2.2 OTROS ACTIVOS

No estipulado.

9.2.3 SEGURO O COBERTURA DE GARANTÍA PARA ENTIDADES FINALES

Según lo dispuesto en la CPS.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN DEL NEGOCIO

9.3.1 TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

Según lo dispuesto en la CPS.

9.3.2 TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Según lo dispuesto en la CPS.

9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Según lo dispuesto en la CPS.

9.4 PRIVACIDAD DE LA INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

Según lo dispuesto en la CPS.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Según lo dispuesto en la CPS.

9.4.3 INFORMACIÓN NO CONSIDERADA PRIVADA

Según lo dispuesto en la CPS.

9.4.4 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN PRIVADA

Según lo dispuesto en la CPS.

9.4.5 AVISO Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Según lo dispuesto en la CPS.

9.4.6 DIVULGACIÓN DE CONFORMIDAD CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Según lo dispuesto en la CPS.

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Según lo dispuesto en la CPS.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

Según lo dispuesto en la CPS.

9.6 OBLIGACIONES Y RESPONSABILIDAD CIVIL

9.6.1 OBLIGACIONES Y RESPONSABILIDAD DE LA AC

Según lo dispuesto en la CPS.

9.6.2 OBLIGACION Y RESPONSABILIDAD DE LA AR

Según lo dispuesto en la CPS.

9.6.3 OBLIGACIÓN Y RESPONSABILIDAD DEL SUSCRIPTOR

9.6.4 *SEGÚN LO DISPUESTO EN LA CPS.*OBLIGACIÓN Y RESPONSABILIDAD DE LA PARTE QUE CONFÍA

Según lo dispuesto en la CPS.

9.6.5 OBLIGACIÓN Y RESPONSABILIDAD DE OTROS PARTICIPANTES

No estipulado.

9.7 EXONERACIÓN DE RESPONSABILIDAD

Según lo dispuesto en la CPS.

9.8 LIMITACIÓN DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

Según lo dispuesto en la CPS.

9.9 INDEMNIZACIONES

Según lo dispuesto en la CPS.

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

Según lo dispuesto en la CPS.

9.10.2 FINALIZACIÓN

Según lo dispuesto en la CPS.

9.10.3 EFECTO DE LA TERMINACIÓN Y SUPERVIVENCIA

Según lo dispuesto en la CPS.

9.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIÓN CON LOS PARTICIPANTES

Según lo dispuesto en la CPS.

9.12 MODIFICACIONES

9.12.1 ROCEDIMIENTO DE MODIFICACIÓN

Según lo dispuesto en la CPS.

9.12.2 MECANISMO DE NOTIFICACIÓN Y PLAZOS

Según lo dispuesto en la CPS.

9.12.3 CIRCUNSTANCIAS EN LAS QUE SE DEBE CAMBIAR EL OID

No estipulado.

9.13 PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS

Según lo dispuesto en la CPS.

9.14 LEGISLACIÓN APLICABLE

Según lo dispuesto en la CPS.

9.15 CONFORMIDAD CON LA LEY APLICABLE

Según lo dispuesto en la CPS.

9.16 CLÁUSULAS DIVERSAS

9.16.1 ACUERDO COMPLETO

Según lo dispuesto en la CPS.

9.16.2 ASIGNACIÓN

Según lo dispuesto en la CPS.

9.16.3 SEPARABILIDAD

Según lo dispuesto en la CPS.

9.16.4 CUMPLIMIENTO (HONORARIOS DE ABOGADOS Y EXENCIÓN DE DERECHOS)

Según lo dispuesto en la CPS.

9.16.5 FUERZA MAYOR

Según lo dispuesto en la CPS.

9.17 OTRAS PROVISIONES

No estipulado.

Apendice 1 Historia del documento

Mayo 2025	V1.0	Creación del documento