



Tinexta Infocert

PDS - TEXTOS DE DIVULGACION DE LOS CERTIFICADOS NO PERSONALES DE CAMERFIRMA

Versión 1.1

Redacción y Revisión: Departamentos de Cumplimiento y Jurídico de Camerfirma

Aprobación (AP): Departamento Jurídico de Camerfirma

Este documento se puede obtener en la dirección:

<https://pds.camerfirma.com/>

Idioma: Castellano

Código: PUB-2025-18-08

INDICE

1 INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CONFIANZA3

1.1 ORGANIZACION3

2 TIPO Y FINALIDAD DE LOS CERTIFICADOS EMITIDOS BAJO LA POLÍTICA DE CERTIFICADOS NO PERSONALES4

3 USOS DEL CERTIFICADO7

3.1 USOS APROPIADOS DE LOS CERTIFICADOS7

3.2 USOS PROHIBIDOS DE LOS CERTIFICADOS7

4 OBLIGACIONES7

4.1 OBLIGACIONES DE CAMERFIRMA.....7

4.2 OBLIGACIONES Y RESPONSABILIDADES DEL SUScriptor, DEL SOLICITANTE Y DEL TITULAR DEL CERTIFICADO8

4.3 OBLIGACIONES DE TERCEROS QUE CONFÍAN EN LOS CERTIFICADOS8

5 LIMITACIÓN DE RESPONSABILIDAD.....9

6 PROTECCION DE DATOS PERSONALES9

7 TARIFAS DE LOS SERVICIOS Y POLITICA DE REEMBOLSO10

8 LEGISLACION APLICABLE10

APENDICE 1 HISTORIA DEL DOCUMENTO11



1 INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CONFIANZA

1.1 ORGANIZACION

Los datos corporativos del Prestador de Servicios de Confianza son:

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>



2 TIPO Y FINALIDAD DE LOS CERTIFICADOS EMITIDOS BAJO LA POLÍTICA DE CERTIFICADOS NO PERSONALES

Camerfirma emite los siguientes tipos de certificados bajo la Política de Certificados dirigidos a personas jurídicas o a objetos:

- **Certificado Cualificado de Sello Electrónico:**

Este certificado cualificado identifica a una persona jurídica (Titular / Creador de un Sello).

El Solicitante de este certificado debe tener facultades de representación que le permitan solicitar el certificado en nombre de la persona jurídica a la que se emite el certificado.

El uso de la clave privada asociada a este certificado dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica.

Este certificado puede estar asociado a una clave privada activada por una máquina o aplicación, para permitir que las operaciones que la usan se realicen de forma automática y desasistida. También se permite como elemento de identificación de máquina o aplicación cliente en protocolos de comunicación electrónica seguros TLS.

- **Certificado Cualificado de Sello Electrónico AAPP**

Este certificado cualificado identifica una persona jurídica del tipo Administración Pública (Titular / Creador de un Sello), conforme a lo establecido en el artículo 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Solicitante de este certificado debe tener facultades de representación que le permitan solicitar el certificado en nombre de la Administración Pública a la que se emite el certificado.

El uso de la clave privada asociada a este certificado dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica.

Este certificado puede estar asociado a una clave privada activada por una máquina o aplicación, para permitir que las operaciones que la usan se realicen de forma automática y desasistida. También se permite como elemento de identificación de máquina o aplicación cliente en protocolos de comunicación electrónica seguros TLS.

Los certificados emitidos bajo estas PC pueden ser usados por los sistemas de firma para la actuación administrativa automatizada, conforme a lo establecido en el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- **Certificado No Cualificado de Firma de Código**

Este certificado no cualificado identifica a una persona jurídica (Titular / Creador de un Sello).

El Solicitante de este certificado debe tener facultades de representación que le permitan



solicitar el certificado en nombre de la persona jurídica a la que se emite el certificado.

Este certificado permite que los desarrolladores apliquen una firma digital sobre código (ActiveX, applets java, macros para Microsoft Office, etc.) estableciendo de esta forma, en dicho código garantías de integridad y autenticidad.

- **Certificado No Cualificado de Sello Electrónico**

Este certificado no cualificado identifica a una persona jurídica (Titular / Creador de un Sello).

El Solicitante de este certificado debe tener facultades de representación que le permitan solicitar el certificado en nombre de la persona jurídica a la que se emite el certificado.

El uso de la clave privada asociada a este certificado dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica.

Este certificado puede estar asociado a una clave privada activada por una máquina o aplicación, para permitir que las operaciones que la usan se realicen de forma automática y desasistida. También se permite como elemento de identificación de máquina o aplicación cliente en protocolos de comunicación electrónica seguros TLS.

- **Certificado No Cualificado de Personal AAPP**

Este certificado no cualificado identifica a una persona jurídica del tipo Administración Pública (Titular / Creador de un Sello).

El Solicitante de este certificado debe tener facultades de representación que le permitan solicitar el certificado en nombre de la persona jurídica a la que se emite el certificado.

El uso de la clave privada asociada a este certificado dota de integridad y autenticidad a los documentos y transacciones sobre los que se aplica.

Este certificado puede estar asociado a una clave privada activada por una máquina o aplicación, para permitir que las operaciones que la usan se realicen de forma automática y desasistida. También se permite como elemento de identificación de máquina o aplicación cliente en protocolos de comunicación electrónica seguros TLS.

- **Certificado No Cualificado OCSP-HSM**

Cada AC Raíz y cada AC Subordinada gestionada por Camerfirma dentro de las jerarquías bajo esta CPS 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.



Los OIDs de estos certificados se pueden consultar en la siguiente tabla:

OID:	Certificado Cualificado de Sello Electrónico Jerarquía CHAMBERS OF COMMERCE ROOT – 2016 AC CAMERFIRMA FOR LEGAL PERSONS – 2016 1.3.6.1.4.1.17326.10.16.2.1.1 QSCD Tarjeta/Token 1.3.6.1.4.1.17326.10.16.2.1.2 No QSCD 1.3.6.1.4.1.17326.10.16.2.1.3 Autenticación 1.3.6.1.4.1.17326.10.16.2.1.4 Firma Certificado Cualificado de Sello Electrónico AAPP Jerarquía CHAMBERS OF COMMERCE ROOT – 2016 AC CAMERFIRMA FOR LEGAL PERSONS – 2016 1.3.6.1.4.1.17326.10.16.2.2.1.3.3.1 Nivel Alto QSCD Tarjeta/Token 1.3.6.1.4.1.17326.10.16.2.2.1.4.3.1 Nivel Medio- No QSCD Jerarquía CHAMBERS OF COMMERCE ROOT – 2008 Camerfirma AAPP II – 2014 1.3.6.1.4.1.17326.1.3.3.2 (no se emiten nuevos certificados) Certificados No Cualificados de Firma de Código Jerarquía CHAMBERS OF COMMERCE ROOT – 2008 Camerfirma Corporate Server II – 2015 1.3.6.1.4.1.17326.10.11.3.1.1 (P12) 1.3.6.1.4.1.17326.10.11.3.1.1 (CSR) Camerfirma Codesign II – 2014 1.3.6.1.4.1.17326.10.12.2 Certificado No Cualificado de Sello Electrónico Jerarquía CHAMBERS OF COMMERCE ROOT – 2008 Camerfirma Corporate Server II – 2015 1.3.6.1.4.1.17326.10.11.3.1.1 (P12) 1.3.6.1.4.1.17326.10.11.3.1.2 (P10) Camerfirma AAPP II – 2014 (No emite nuevos certificados) 1.3.6.1.4.1.17326.1.3.3.2 Certificados No cualificados de OCSP 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/practic-de-certificacion-ac-camerfirma-CPS-CPS/



3 USOS DEL CERTIFICADO

3.1 USOS APROPIADOS DE LOS CERTIFICADOS

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

- Autenticación del Firmante.
- Sello electrónico cualificado o sello electrónico avanzado, dependiendo de si el certificado está emitido en dispositivo cualificado de creación firma electrónica o no.
- Integridad del documento sellado: La utilización de estos certificados garantiza que el documento firmado es íntegro, es decir, que el documento no fue alterado o modificado después de firmado por el Firmante/Suscriptor
- Cifrado asimétrico o mixto sin recuperación de clave, bajo la responsabilidad del titular/suscriptor

3.2 USOS PROHIBIDOS DE LOS CERTIFICADOS

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

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.

4 OBLIGACIONES

4.1 OBLIGACIONES DE CAMERFIRMA

Camerfirma, como Prestador de Servicios de Confianza que emite certificados, esta obligada a lo siguiente:

- a) Publicar información veraz y actualizada.
- b) Gestionar la emisión, entrega y revocación de los certificados por sí o a través de sus Autoridades de Registro (RA)
- c) Ejecutar los servicios con los medios técnicos y materiales y personales adecuados, con la cualificación profesional requerida.
- d) Cumplir los niveles de calidad en los servicios de acuerdo con los establecido en la CPS en



cuanto a los aspectos técnicos, operativos y de seguridad.

- e) Notificar al suscriptor, antes de la fecha de vencimiento, de la posibilidad de renovación de su certificado, así como su revocación, si procede.
- f) Disponer de servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.
- g) Conservar la información relativa a la emisión del certificado durante 15 años desde la extinción del certificado.

4.2 OBLIGACIONES Y RESPONSABILIDADES DEL SUSCRIPTOR, DEL SOLICITANTE Y DEL TITULAR DEL CERTIFICADO

- a) Cumplir con la normativa aplicable, la Declaración de Prácticas de Certificación (CPS) y la Política de Certificación (CP) y, en su caso, los documentos contractuales firmados con la AC y/o la AR.
- b) Aceptar los Términos y Condiciones Generales del servicio.
- c) Suministrar a la AC la información necesaria para realizar una correcta identificación
- d) Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- e) Custodiar su clave privada de manera diligente
- f) Informar de la existencia de alguna causa de revocación.
- g) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- h) No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación

4.3 OBLIGACIONES DE TERCEROS QUE CONFÍAN EN LOS CERTIFICADOS

Los terceros que confían en un certificado emitido por Camerfirma deberán:

- a) Verificar la validez de los certificados que se presentan por los firmantes.
- b) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía.
- c) Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la PC pertinente.
- d) Notificar a Camerfirma cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.



5 LIMITACIÓN DE RESPONSABILIDAD

Camerfirma no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si esta incurre en alguno de los supuestos siguientes:

- a) No haber proporcionado a Camerfirma información veraz, completa y exacta para la emisión del certificado, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia.
- b) La falta de comunicación sin demora indebida a Camerfirma de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.
- c) Negligencia en la conservación de sus datos de creación de firma.
- d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o Camerfirma le notifique la extinción o suspensión de su vigencia.
- f) No comprobar la revocación o pérdida de vigencia del certificado, o no verifique la firma por parte de las partes que confían.
- g) Camerfirma no será responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público.

6 PROTECCION DE DATOS PERSONALES

Camerfirma cumple con la normativa vigente en cada momento en materia de protección de datos, en particular, ha adaptado sus procedimientos al REGLAMENTO (UE) 2016/679 General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La información personal que no está públicamente disponible en el contenido de un certificado o CRL se considera 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.

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.



7 TARIFAS DE LOS SERVICIOS Y POLITICA DE REEMBOLSO

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.

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

8 LEGISLACION 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.

Apendice 1 Historia del documento

Marzo 2016	V 1.0	Creación del documento
Abril 2025	V 1.1	Actualización del documento

