Tinexta Infocert

POLÍTICA DE CERTIFICACIÓN

PARA CERTIFICADOS NO PERSONALES

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-2025-18-13

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2025.05.29 15:46:32 +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.

la presente PC establece los requisitos, normas y procedimientos aplicables a la emisión, uso, gestión y revocación de certificados electrónicos no personales (de sello electrónico, de firma de código y de OCSP) 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.

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 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 maquina o aplicación cliente en protocolos de comunicación electrónica seguros TLS.

  Camerfirma emite estos certificados cualificados en dispositivos seguros de creación de firma - QSCD (tarjeta o token criptográfico) bajo el OID 0.4.0.194112.1.3 según ETSI EN 319 411-2 – QCP-l-qscd, y en dispositivos No QSCD bajo el OID 0.4.0.194112.1.1 según ETSI EN 319 411-2 - QCP-l

- **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 maquina 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.

Los certificados emitidos bajo estas PC son conformes a la normativa nacional del perfil de certificado de sello electrónico de la Administración Pública establecido en el apartado 9 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 su nivel alto: OID 2.16.724.1.3.5.6.1
- en su nivel medio/sustancial: OID 2.16.724.1.3.5.6.2

Camerfirma emite estos certificados cualificados en dispositivos seguros de creación de firma - QSCD (tarjeta o token criptográfico) bajo el OID 0.4.0.194112.1.3 según ETSI EN 319 411-2 – QCP-l-qscd, y en dispositivos No QSCD bajo el OID 0.4.0.194112.1.1 según ETSI EN 319 411-2 - QCP-l.

- **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 maquina o aplicación cliente en protocolos de comunicación electrónica seguros TLS.

- **Certificado No Cualificado de Sello Electrónico 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 maquina 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.

- **Certificado Cualificado de TSU**

  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.

  Este certificado puede ser usado para la firma digital de sellos de tiempo emitidos por una TSU.

  Las claves de este certificado se generan y almacenan en un HSM QSCD, conforme a los requisitos establecidos en ETSI EN 319 421.

1.2 IDENTIFICACIÓN Y NOMBRE DEL DOCUMENTO

Nombre:	Política de Certificación para certificados NO personales de CAMERFIRMA

Descripción:	Políticas de Certificación para certificados NO personales de CAMERFIRMA: certificados de sello electrónico, certificados de firma de código y certificados OCSP.
Versión:	Ver página inicial
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) • **CP TSU Qualified Certificate** Jerarquía CHAMBERS OF COMMERCE ROOT – 2016 AC CAMERFIRMA TSA - 2016 ○ 1.3.6.1.4.1.17326.10.16.5.1.1 - QSCD HSM (no new certificates are issued) Jerarquía INFOCERT-CAMERFIRMA TIMESTAMP 2024 INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024 ○ 1.3.6.1.4.1.17326.10.21.30.4 - QSCD HSM • **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/practicas-de-certificacion-ac-camerfirma-CPS-CPS/

Anteriormente, esta Política estaba contenida en la CPS 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 CPS, 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 2016:
  - AC CAMERFIRMA FOR LEGAL PERSONS – 2016
  - AC CAMERFIRMA TSA - 2016
- CHAMBERS OF COMMERCE ROOT 2008:
  - Camerfirma Codesign II – 2014
  - Camerfirma Corporate Server II – 2015
  - Camerfirma AAPP II – 2014
- CAMERFIRMA ROOT 2021:
  - AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021
- INFOCERT-CAMERFIRMA TIMESTAMP - 2024
  - INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024

1.3.1.1 CERTIFICADOS DE PRUEBAS

Según lo dispuesto en la CPS.

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 CP, 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.

  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 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:

- La Entidad (persona jurídica) Titular.
- La Entidad (persona jurídica) identificada en el certificado a la que está vinculada el Titular, en los casos en los que el Titular no es la Entidad.
- Una persona jurídica con facultades de representación de la Entidad (persona jurídica) Titular.
- Una persona jurídica con facultades de representación de la Entidad (persona jurídica) identificada en el certificado a la que está vinculada el Titular, en los casos en los que el Titular no es la Entidad.

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

- Una tercera organización que actúe como AR bajo esta CPS 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:

- La Entidad (persona jurídica) a la que se emite el certificado. El Suscriptor es la Entidad Titular (la persona jurídica identificada en el certificado) u otra persona jurídica con facultades de representación de la Entidad Titular.
- Una organización, unidad, área o departamento vinculado a la Entidad (persona jurídica) a la que se emite el certificado. El Suscriptor es la Entidad identificada en el certificado a la que está vinculado el Titular (la persona jurídica identificada en el certificado) u otra persona jurídica con facultades de representación de la Entidad identificada en el certificado a la que está vinculado el Titular.
- Un dispositivo, aplicación o sistema operado por o en nombre de la Entidad (persona jurídica) a la que se emite el certificado. El Suscriptor es la Entidad identificada en el certificado a la que está vinculado el Titular (la persona jurídica identificada en el certificado) u otra persona jurídica con facultades de representación de la Entidad identificada en el certificado a la que está vinculado el Titular.

Bajo esta PC, y de acuerdo con el Reglamento eIDAS, el **Creador de un Sello** es la persona jurídica identificada en un certificado de sello electrónico, que puede ser:

- Si el Titular es la Entidad (persona jurídica) a la que se emite el certificado, el Creador de un Sello es la Entidad (persona jurídica), el Titular y, en su caso, el Suscriptor.
- Si el Titular es una organización, unidad, área o departamento vinculado a la Entidad (persona jurídica) a la que se emite el certificado, el Creador de un Sello es la Entidad (persona jurídica) a la que está vinculada el Titular y, en su caso, el Suscriptor.
- Si el Titular es un dispositivo, aplicación o sistema operado por o en nombre de la Entidad (persona jurídica) a la que se emite el certificado, el Creador de un Sello es la Entidad (persona jurídica) a la que está vinculada el Titular y, en su caso, el Suscriptor.

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.

1.3.3.3 SOLICITANTE

Bajo estas PC, el Solicitante de un certificado será la persona física que solicita un certificado para la persona jurídica a la que representa.

Bajo estas PC, el Solicitante de un certificado puede ser una persona física con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica) a la que se emite el certificado.

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 Creador de un Sello y, en su caso, del Titular.

1.3.5 ENTIDAD

Bajo esta PC, 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.

Bajo estas PC, la Entidad de un certificado puede ser la persona jurídica identificada en el certificado, que puede ser:

- Si el Titular es la Entidad (persona jurídica) a la que se emite el certificado, el Titular, Suscriptor y Creador de un Sello.
- Si el Titular es una organización, unidad, área o departamento vinculado a la Entidad (persona jurídica) a la que se emite el certificado, el Suscriptor y Creador de un Sello.
- Si el Titular es un dispositivo, aplicación o sistema operado por o en nombre de la Entidad (persona jurídica) a la que se emite el certificado, el Suscriptor y Creador de un Sello.

1.3.6 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.

1.3.7 OTROS PARTICIPANTES

1.3.7.1 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.
- Sello electrónico avanzado, o sello electrónico cualificado cuando se utilicen con dispositivos cualificados de creación de sellos electrónicos.

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 CPS, 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 CPS 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-CPS/
- 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 jurídicas, excepto para los certificados de TSU y OCSP:
    - Si el Titular es la Entidad (persona jurídica) a la que se emite el certificado:
        - Denominación social e identificador fiscal de la Entidad.
        - País donde realiza la actividad la persona jurídica propietaria (C).
    - Si el Titular es una organización, unidad, área o departamento vinculado a la Entidad (persona jurídica) a la que se emite el certificado:
        - Denominación social e identificador fiscal de la Entidad.
        - Unidad, área o departamento.
        - País donde realiza la actividad la persona jurídica propietaria (C).
    - Si el Titular es un dispositivo, aplicación o sistema operado por o en nombre de la Entidad (persona jurídica) a la que se emite el certificado:
        - Denominación social e identificador fiscal de la Entidad.
        - Nombre del dispositivo, aplicación o sistema.
        - País donde realiza la actividad la persona jurídica propietaria (C).
- Para los certificados de AC, de TSU y OCSP (emitidos a personas jurídicas), en el DN en el campo *Subject*:
    - Nombre descriptivo de la AC, la TSU o el servicio OCSP (*CN*).
    - Denominación social de la persona jurídica propietaria (O).
    - Identificador fiscal de la persona jurídica propietaria (*organizationIdentifier* y/o *serialNumber*).
    - País donde realiza la actividad la persona jurídica propietaria (C).

Las fichas de los perfiles de certificados bajo estas CPS y 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

En estos tipos de certificados no se admiten pseudónimos de los suscriptores.

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

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 un certificado emitido por una AC de Camerfirma o de otro PCSC, siempre que contengan los datos de identidad del solicitante.

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.

3.2.1 MÉTODOS DE PRUEBA DE LA POSESIÓN DE LA CLAVE PRIVADA

Según lo dispuesto en la CPS

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 de Sello Electrónico	En el caso de que el Solicitante y el Responsable sean personas distintas, autorización firmada por el Solicitante (autorizante) al Responsable (autorizado), para que solicite y se le entregue el certificado y haga uso de él. Certificado o consulta al Registro Mercantil para comprobar la constitución y personalidad jurídica de la Entidad, y el nombramiento y vigencia del cargo del Solicitante (en su caso, a la vez, autorizante) con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica).
Certificado Cualificado de Sello Electrónico AAPP	En el caso de que el Solicitante y el Responsable sean personas distintas, autorización firmada por el Solicitante (autorizante) al Responsable (autorizado), para que solicite y se le entregue el certificado y haga uso de él. Certificado para comprobar el nombramiento y vigencia del cargo del Solicitante (en su caso, a la vez, autorizante) con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica), o nombramiento del Solicitante en Boletín Oficial donde conste el DNI/NIE de esta persona.
Certificado Cualificado de TSU Certificado No Cualificado de Firma de Código	En el caso de que el Solicitante y el Responsable sean personas distintas, autorización firmada por el Solicitante (autorizante) al Responsable (autorizado), para que solicite y se le entregue el certificado y haga uso de él. En el caso de que la Entidad no sea una Administración Pública, certificado o consulta al Registro Mercantil para comprobar la constitución y personalidad jurídica de la Entidad, y el nombramiento y vigencia del cargo Solicitante (en su caso, a la vez, del

				autorizante) con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica). En el caso de que la Entidad sea una Administración Pública, certificado para comprobar el nombramiento y vigencia del cargo del Solicitante (en su caso, a la vez, autorizante) con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica), o nombramiento del Solicitante en Boletín Oficial donde conste el DNI/NIE de esta persona.
Certificado No Electrónico	No	Cualificado	de	Sello	En el caso de que el Solicitante y el Responsable sean personas distintas, autorización firmada por el Solicitante (autorizante) al Responsable (autorizado), para que solicite y se le entregue el certificado y haga uso de él. Certificado para comprobar el nombramiento y vigencia del cargo del Solicitante (en su caso, a la vez, autorizante) con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica), o nombramiento del Solicitante en Boletín Oficial donde conste el DNI/NIE de esta persona.
Certificado No Electrónico AAPP	No	Cualificado	de	Sello	En el caso de que el Solicitante y el Responsable sean personas distintas, autorización firmada por el Solicitante (autorizante) al Responsable (autorizado), para que solicite y se le entregue el certificado y haga uso de él. Certificado para comprobar el nombramiento y vigencia del cargo del Solicitante (en su caso, a la vez, autorizante) con facultades de representación que le permitan solicitar el certificado en nombre de la Entidad (persona jurídica), o nombramiento del Solicitante 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 notifica 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 LEGAL PERSONS - 2016	critical, cRLSign, keyCertSign	emailProtection clientAuth	critical, CA:true, pathLen:2
Certificado Cualificado de Sello Electrónico - QSCD Tarjeta/Token, No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado de Sello Electrónico AAPP - Nivel Alto - QSCD Tarjeta/Token	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false
Certificado Cualificado de Sello Electrónico AAPP - Nivel Medio - No QSCD	critical, digitalSignature, contentCommitment, keyEncipherment	emailProtection clientAuth	critical, CA:false

Certificado Cualificado de Sello Electrónico Autenticación	digitalSignature	clientAuth	
Certificado Cualificado de Sello Electrónico Firma	nonRepudiation	-	critical, CA:false
Chambers of Commerce Root – 2008 (certificado SHA-1)	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:12
Chambers of Commerce Root – 2008 (certificado SHA -256)	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:12
Camerfirma Codesign II - 2014	critical, cRLSign, keyCertSign	codesigning msCodeCom	critical, CA:true, pathLen:2
Certificado No Cualificado de Firma de Código	critical, digitalSignature, nonRepudiation	codesigning msCodeCom	critical, CA:false
Camerfirma Corporate Server II - 2015	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical, CA:true, pathLen:2
Certificado No Cualificado de Sello Electrónico - P12, P10	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement	clientAuth emailProtection	critical, CA:false
Camerfirma AAPP II - 2014	critical, cRLSign, keyCertSign	emailProtection clientAuth serverAuth	critical, CA:true, pathLen:2
Certificado No Cualificado de Sello Electrónico APPP	critical, digitalSignature, contentCommitment, keyEncipherment, dataEncipherment	clientAuth emailProtection	critical, CA:false
GLOBAL CHAMBERSIGN ROOT - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true
AC CAMERFIRMA COLOMBIA - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:2
AC CAMERFIRMA PERÚ - 2016	critical, cRLSign, keyCertSign	-	critical, CA:true, pathLen:2
CAMERFIRMA ROOT 2021	critical, cRLSign,	-	critical, CA:true

	keyCertSign		
AC CAMERFIRMA QUALIFIED CERTIFICATES – 2021	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0
Certificado No Cualificado OCSP	critical, digitalSignature, nonRepudiation	OCSPSigning	critical, CA:false
INFOCERT-CAMERFIRMA TIMESTAMP 2024	critical, cRLSign, keyCertSign	-	critical, CA:true
INFOCERT-CAMERFIRMA QUALIFIED TSA - 2024	critical, cRLSign, keyCertSign	emailProtection, clientAuth	critical, CA:true, pathLen:0
TSU Qualified Certificate - QSCD HSM	critical, contentCommitment,	timeStamping	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 sello remoto, el Titular / Creador de un Sello debe conservar las herramientas y/o dispositivos de autenticación del sello remoto de forma segura. Asimismo, debe mantener el PIN de activación de la clave privada del certificado de sello remoto bajo su control 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 / Creador de un Sello no deben crear sellos 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 5 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