

DECLARACIÓN DE PRÁCTICAS DE REGISTRO



Camerfirma

Certificado Digital

CAMERFIRMA PERÚ ENTIDAD DE REGISTRO Versión 1.0

Idioma: **Castellano**

Fecha: **abril 2017**

Estado del documento: **Activo**

Información sobre el documento

Nombre: Declaración de Prácticas de Registro de Camerfirma Perú

Código

Versión: 1.0.

Elaborado por: ER Camerfirma Perú

Idioma: Castellano

Descripción: Define los criterios básicos a seguir por el prestador de servicios de certificación que ofrezca servicios de Entidad de Registro.

Fecha de edición: Abril 2017

Estado del documento: Activo

Localización: <http://www.camerfirma.com/>

Control de versiones

VERSIÓN	MOTIVACIÓN DEL CAMBIO	FECHA
V.1.0	Elaboración de los documentos normativos para Camerfirma Perú como Entidad de Registro.	Abr 2017

Índice de Contenido

1. Introducción	9
1.1. Vista General	9
1.2. Identificación	10
1.3. Comunidad y Ámbito de Aplicación	10
1.3.1 Entidad de Certificación	10
1.3.2 Entidad de Registro	10
1.3.3 Proveedor de servicios e infraestructura	10
1.3.4 Titular	10
1.3.5 Suscriptor	11
1.3.6 Parte Usuaría	11
1.3.7 Solicitante	11
1.4. Usos del certificado digital	11
1.4.1 Ámbito de Aplicación y Usos	11
1.4.2 Usos Prohibidos y no Autorizados	12
2. Cláusulas Generales	13
2.1. Obligaciones	13
2.1.1 Entidad de Registro	13
2.1.2 Solicitante	14
2.1.3 Suscriptor	14
2.1.4 Parte usuaria	14
2.2. Responsabilidad	15
2.2.1 Responsable de los documentos de la ER	15
2.2.2 Exoneración de responsabilidad	15
2.2.3 Límite de responsabilidad en caso de pérdidas por transacciones	16
2.3. Responsabilidad financiera	16
2.4. Interpretación y ejecución	16
2.4.1 Legislación	16
2.4.2 Independencia	16
2.4.3 Notificación	16
2.4.4 Procedimiento de resolución de disputas	16
2.5. Tarifas	17
2.5.1 Tarifas de emisión de certificados y renovación	17
2.5.2 Tarifas de acceso a los certificados	17
2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados	17
2.5.4 Tarifas por el acceso al contenido de estas Políticas de Certificación	17
2.5.5 Política de reintegros	17
2.6. Políticas y Prácticas de Certificación	17
2.6.1 Declaración de Prácticas	17

2.6.2	Declaración Informativa	18
2.7.	Publicación y repositorios	18
2.7.1	Publicación de información de la AC	18
2.7.2	Frecuencia de publicación	19
2.7.3	Controles de acceso a los repositorios	19
2.8.	Auditorías	19
2.8.1	Frecuencia de las auditorías	19
2.8.2	Identificación y cualificación del auditor	20
2.8.3	Relación entre el auditor y la ER	20
2.9.	Confidencialidad	20
2.9.1	Tipo de información a mantener confidencial	20
2.9.2	Tipo de información considerada no confidencial	21
2.9.3	Divulgación de información de revocación de certificados	21
2.9.4	Envío a la Autoridad Competente	21
2.10.	Derechos de propiedad intelectual	21
3.	<i>Especificación de la Administración</i>	22
3.1.	Autoridad de las políticas	22
3.2.	Procedimientos de especificación de cambios	22
3.3.	Procedimientos de aprobación de la DPC	22
4.	<i>Solicitud de Emisión de certificados digitales</i>	23
4.1.	Solicitud de certificados a persona jurídica	23
4.1.1	Servicios brindados	23
4.1.2	Autorizadas para realizar la solicitud	23
4.1.3	Modalidades de atención	24
4.1.4	Solicitud de certificados de atributos	24
4.1.5	Solicitud de certificados para agentes automatizados	24
4.1.6	Reconocimiento, autenticación y rol de las marcas registradas	24
4.1.7	Identificación y autenticación de solicitantes de certificados de persona jurídica	25
4.1.8	Contrato del titular	25
4.1.9	Verificación de suscriptores	25
4.2.	Solicitud de certificados de persona natural	26
4.2.1	Servicios brindados	26
4.2.2	Autorizados para realizar la solicitud	26
4.2.3	Modalidades de atención	26
4.2.4	Solicitud de certificados de persona natural	26
4.2.5	Contrato del suscriptor	26
4.2.6	Verificación de suscriptores	27
4.2.7	Identificación y autenticación de solicitantes de certificados de persona natural	27
5.	<i>Procesamiento de la solicitud</i>	27

5.1.	Rechazo de la solicitud de emisión de un certificado	27
5.2.	Aprobación de la solicitud de emisión de un certificado	28
5.3.	Registro de documentos	28
5.4.	Método para probar la posesión de la clave privada	28
5.5.	Tiempo para el procesamiento de la solicitud de un certificado	28
5.6.	Emisión del certificado	28
6.	<i>Solicitud de re-emisión de certificados digitales</i>	29
6.1.	Solicitud de re-emisión certificados de persona jurídica	29
6.1.1	Servicios brindados	29
6.1.2	Autorizados para realizar la solicitud	29
6.1.3	Modalidades de atención	30
6.1.4	Solicitud de re-emisión de certificados de atributos	30
6.1.5	Solicitud de re-emisión de certificados para agentes automatizados	30
6.1.6	Identificación y autenticación de solicitantes de re-emisión de certificados de persona jurídica	30
6.2.	Solicitud de re-emisión de certificados de persona natural	31
6.2.1	Servicios brindados	31
6.2.2	Autorizados para realizar la solicitud	31
6.2.3	Modalidades de atención	31
6.2.4	Solicitud de certificados de persona natural	31
6.2.5	Identificación y autenticación de solicitantes de certificados de persona natural	31
7.	<i>Procesamiento de la solicitud de re-emisión</i>	32
7.1.	Rechazo de la solicitud de emisión de un certificado	32
7.2.	Aprobación de la solicitud de emisión de un certificado	32
7.3.	Registro de documentos	32
7.4.	Método para probar la posesión de la clave privada	33
7.5.	Tiempo para el procesamiento de la solicitud de un certificado	33
7.6.	Re-emisión del certificado	33
8.	<i>Solicitud de revocación de certificados</i>	33
8.1.	Circunstancias para realizar la solicitud	33
8.2.	Solicitud de revocación de certificados	33
8.2.1	Servicios brindados	33

8.2.2	Autorizados para realizar la solicitud	34
8.2.3	Identificación y autenticación de los solicitantes	34
8.2.4	Modalidades de atención	35
8.2.5	Solicitud de revocación de certificados de atributos	35
8.2.6	Solicitud de revocación de certificados para agentes automatizados	35
8.2.7	Solicitud de revocación de certificados de persona natural	35
9.	Procesamiento de la solicitud de revocación	36
9.1.	Rechazo de la solicitud de revocación emisión de un certificado	36
9.2.	Aprobación de la solicitud de revocación de un certificado	36
9.3.	Registro de documentos	36
9.4.	Tiempo para el procesamiento de la solicitud de revocación	37
9.5.	Revocación del certificado	37
10.	Gestión de la seguridad	37
11.	Gestión de Operaciones	37
11.1.	Módulo criptográfico	37
11.2.	Restricciones de la generación de claves	37
11.3.	Entrega de la clave pública	37
11.4.	Depósito de clave privada	37
11.5.	Datos de activación	38
12.	Controles de seguridad computacional	38
13.	Auditorías	¡Error! Marcador no definido.
13.1.	Frecuencias de auditorías	¡Error! Marcador no definido.
13.2.	Calificaciones de los auditores	¡Error! Marcador no definido.
13.3.	Relación del auditor con la ER	¡Error! Marcador no definido.
14.	Materias de negocio y legales	38
14.1.	Tarifas	38
14.2.	Políticas de reembolso	38
14.3.	Cobertura de seguro	38
14.4.	Provisiones y garantías	38
14.5.	Excepciones de garantías	38
14.6.	Obligaciones de los suscriptores y titulares	38
14.7.	Obligaciones de los terceros que confían	39

14.8.	Indemnización	39
14.9.	Notificaciones	39
14.10.	Enmendaduras y cambios	39
14.11.	Resolución de disputas	39
14.12.	Conformidad con la Ley aplicable	39
14.13.	Subrogación	39
14.14.	Fuerza mayor	39
14.15.	Derechos de propiedad intelectual	39
	definido.	
15.	<i>Cumplimiento de requerimientos legales</i>	40
16.	<i>Conformidad</i>	41
	<i>Anexo I. Acrónimos</i>	42
	<i>Anexo II. Definiciones</i>	44

1. Introducción

AC Camerfirma S.A. (Camerfirma España) es una empresa que fue creada en el año 1999 con domicilio en España, donde se establece como prestador de servicios de certificación al amparo de la LEY 59/2003, de 19 de diciembre, de firma electrónica en España.

Camerfirma España, como entidad líder española en la emisión de certificados empresariales en el sector privado tiene mucho que ofrecer en cuanto a conocimiento de esta tecnología a nivel europeo e incluso mundial. Camerfirma España desde el comienzo de su trayectoria como sociedad anónima en el año 2000, mantiene una estrecha relación con los mercados de Sudamérica y cuenta en su labor con numerosos proyectos de consultoría y de implantación de PKI con las Cámaras de Comercio sudamericanas.

En el año 2014, Camerfirma logró acreditarse como Entidad de Certificación en Perú bajo el nombre de Camerfirma Perú S.A. (Camerfirma Perú). En el año 2017, se acreditó como Entidad de Registro, prestador de servicios de intermediación digital y servicios de emisión de Sellos de Tiempo (Timestamp), para brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

La infraestructura tecnológica y operativa de la EC de Camerfirma Perú es provista y administrada por Camerfirma España. Dicha infraestructura ha obtenido la certificación Webtrust for Certification Authorities, y es verificada anualmente por auditores autorizados.

Camerfirma Perú, como ER, brinda los servicios de registro o verificación de sus clientes a través de su oficina en Perú, tanto en el caso de personas jurídicas como naturales.

1.1. Vista General

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza Camerfirma Perú para la administración de sus servicios como Entidad de Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Entidades de Registro o Verificación– ER” establecida por el INDECOPI, en calidad de Autoridad Administrativa Competente de la Infraestructura Oficial de la Firma Electrónica del Perú.

1.2. Identificación

Nombre de la Política:	Declaración de Prácticas de Registro de Camerfirma Perú
Descripción:	
Versión:	1.0
Fecha de Emisión:	abril de 2017
Localización:	http://www.camerfirma.com/

1.3. Comunidad y Ámbito de Aplicación

Este documento puede ser utilizado por terceros receptores de certificados digitales de Camerfirma Perú y suscriptores del servicio de emisión de certificados digitales como base para confirmar la fiabilidad de los servicios descritos en él.

1.3.1 Entidad de Certificación

Camerfirma Perú, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

A Camerfirma Perú, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la ACC a fin de poder ingresar a la IOFE.

1.3.2 Entidad de Registro

Camerfirma Perú brinda los servicios de Entidad de Registro, la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

1.3.3 Proveedor de servicios e infraestructura

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación de Camerfirma Perú, cuando la entidad de certificación así lo requiere y garantizan la continuidad del servicio a los titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece Camerfirma Perú son provistos por Camerfirma España.

1.3.4 Titular

1.3.5 Suscriptor

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

1.3.6 Parte Usuaría

En esta Política se entiende por Parte Usuaría a la persona que voluntariamente confía en los sellos de tiempo emitidos bajo esta política y se sujeta a lo dispuesto en ella por lo que no se requerirá acuerdo posterior alguno.

La Parte Usuaría también puede denominarse como "Tercero que Confía".

1.3.7 Solicitante

Se entenderá por Solicitante, la persona natural o jurídica que solicita un certificado emitido bajo esta RPS.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

1.4. Usos del certificado digital

1.4.1 Ámbito de Aplicación y Usos

Los certificados emitidos bajo la Declaración de Prácticas de Camerfirma Perú pueden ser utilizados para los siguientes propósitos:

- Identificación del Titular que firma un documento o que se autentica para acceder a un sistema: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el certificado.
- Integridad del documento firmado: La utilización del certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.
- No repudio de origen: Con el uso de este certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

1.4.2 Usos Prohibidos y no Autorizados

Bajo la presente Política no se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en este documento y en la Declaración de Prácticas de Certificación.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la EC.

2. Cláusulas Generales

2.1. Obligaciones

Este apartado incluye todas las obligaciones, garantías y responsabilidades de la ER frente a los usuarios y terceras partes que voluntariamente confían en los servicios de sellado de tiempo, así como las obligaciones asumidas por las partes.

2.1.1 Entidad de Registro

Las ER son las entidades delegadas por la EC para realizar las tareas de registro y aprobación de las solicitudes de certificados, por lo tanto, la ER también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

- Respetar lo dispuesto en la CPS y en la Política de Certificación correspondiente.
- Proteger sus claves privadas que les servirán para el ejercicio de sus funciones.
- Comprobar la identidad de los Sujetos/Firmantes y Solicitantes de los certificados cuando resulte necesario, acreditando definitivamente la identidad del Firmante, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de organización, de acuerdo con lo establecido en las secciones correspondientes de el documento CPS.
- Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- Proporcionar al Firmante, en caso de certificados individuales, o al futuro poseedor de claves, en caso de certificados de organización, acceso al certificado.
- Entregar, en su caso, el dispositivo criptográfico correspondiente.
- Archivar, por el periodo dispuesto en la legislación vigente, los documentos suministrados por el solicitante o Firmante.
- Respetar lo dispuesto en los contratos firmados con Camerfirma España y con el Sujeto/Firmante.
- Informar a Camerfirma de las causas de revocación, siempre y cuando tomen conocimiento.
- Ofrecer información básica sobre la política y uso del certificado, incluyendo especialmente información sobre Camerfirma y la Declaración de Prácticas de Certificación aplicable, así como de sus obligaciones, facultades y responsabilidades.
- Ofrecer Información sobre el certificado y el dispositivo criptográfico.
- Recopilar información y evidencias del poseedor de recibir el certificado y, en su caso, el dispositivo criptográfico, y aceptación de dichos elementos.
- Informar del método de imputación exclusiva al poseedor de la clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico,

2.1.2 Solicitante

El solicitante de un certificado digital estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

1. Respetar lo dispuesto en esta política de certificación.
2. Suministrar a la ER la información necesaria para realizar una correcta identificación.
3. Confirmar la exactitud y veracidad de la información suministrada.
4. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

2.1.3 Suscriptor

El suscriptor para hacer uso del certificado digital, asume la obligación de conocer y comprender plenamente las características y limitaciones determinadas en esta Declaración de Prácticas de Certificación y de las Políticas y contratos comerciales vinculados.

El suscriptor de un certificado estará obligado a:

1. Respetar lo dispuesto en el presente documento.
2. Proteger sus claves privadas de forma segura.
3. Emitir el certificado digital conforme a esta Política y a los estándares de aplicación.

2.1.4 Parte usuaria

Las terceras partes que voluntariamente confíen en los certificados digitales (Partes Usuarias) asumen la obligación de:

- Verificar el estado de activación en que se encuentra el certificado digital, mediante consulta a la CRL u otro medio que se disponga para la verificación de estado del certificado.
- En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:
 - La fecha de revocación o de caducidad es posterior a la fecha en que se emitió el certificado.
 - La función criptográfica que se empleó sigue siendo segura.
 - Que la longitud de la Clave criptográfica y el algoritmo de firma electrónica siguen siendo de práctica habitual.
- Tener en cuenta cualquier limitación en el uso del certificado digital indicado en la política o en las prácticas de certificación correspondientes.
- Tomar en consideración cualquier límite prescrito en otros acuerdos de servicio.

2.2. Responsabilidad

La ER será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. La exactitud de toda la información contenida los certificados emitidos.
2. La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
3. Cualquier responsabilidad que se establezca por la legislación vigente.

Camerfirma España, como proveedor de infraestructura y gestión de operaciones de los servicios de la EC de Camerfirma Perú, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC de Camerfirma Perú.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por Camerfirma España de acuerdo a su documento Declaración de Prácticas de Certificación, publicado en:

www.camerfirma.com

Camerfirma Perú es responsable de exigir y supervisar las operaciones de los servicios que son administrados por Camerfirma España.

Como Entidad de Registro, es responsable de la correcta identificación de las personas naturales o jurídicas y de la seguridad en la entrega de certificados digitales, siempre que esta sea realizada por los Operadores de Registro autorizados.

Las peticiones, quejas o reclamos sobre los servicios prestados por Camerfirma Perú a través de Camerfirma España son recibidas directamente por Camerfirma Perú como prestador de servicios digitales o a través de la Entidad de Registro. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone Camerfirma Perú es permanente. Estos reclamos serán comunicados en un lapso no mayor de 5 días a Camerfirma España, para su debida atención.

2.2.1 Responsable de los documentos de la ER

Nombre: Xavier Urios

Cargo: Gerente General de Camerfirma Perú

Dirección de correo electrónico: xurios@cocep.org.pe

2.2.2 Exoneración de responsabilidad

La ER no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
2. Por el uso de los certificados digitales siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Declaración de Prácticas.
3. Por el uso indebido o fraudulento de los certificados digitales emitidos por Camerfirma Perú.
4. Por el uso de la información contenida en el certificado o en la CRL.

5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o usuario en la normativa vigente, en la presente Declaración de Prácticas, en las Políticas Correspondientes o en los contratos establecidos por las partes.
6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.
7. Fraude en la información presentada por el solicitante.

2.2.3 Límite de responsabilidad en caso de pérdidas por transacciones

La ER no se responsabilizará por las pérdidas por transacciones.

2.3. Responsabilidad financiera

La ER no asume ningún tipo de responsabilidad financiera.

Podrán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

2.4. Interpretación y ejecución

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de las presentes Prácticas se regirá por lo dispuesto en la legislación vigente aplicable.

2.4.2 Independencia

La invalidez de una de las cláusulas contenidas en esta Declaración de Prácticas no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

2.4.3 Notificación

Cualquier notificación referente a la presente Declaración de Prácticas se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

2.4.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

2.5. Tarifas

2.5.1 Tarifas de emisión de certificados

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los usuarios en la página Web de Camerfirma <http://www.camerfirma.com/certificados>. No obstante, los precios son referenciales y pueden variar de acuerdo a cada cliente.

2.5.2 Tarifas de acceso a los certificados

Sin estipular.

2.5.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

Camerfirma Perú proveerá de un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito.

2.5.4 Tarifas por el acceso al contenido de estas Políticas de Certificación

El acceso al contenido de la presente Política de Certificación será gratuito.

2.5.5 Política de reintegros

Sin estipular.

2.6. Políticas y Prácticas de Certificación

2.6.1 Declaración de Prácticas

Camerfirma Perú demostrará que cuenta con la fiabilidad necesaria para la provisión del servicio de emisión de certificados digitales.

En particular:

- Dispondrá de un análisis de riesgos para evaluar los activos de empresa y las amenazas de tal forma que determine si son necesarios controles de seguridad u operativos para protegerlos.
- Dispondrá de una Declaración de Prácticas y procedimientos usados para dar respuesta a todos los requerimientos expuestos en estas políticas.
- La Declaración de Prácticas identificará las obligaciones de todos los agentes (internos y externos) implicados en el soporte al servicio de la emisión de certificados digitales.
- La EC pondrá a disposición de suscriptores y usuarios la Declaración de Prácticas y cualquier documentación relevante que garantice la conformidad con esta política. La EC no tiene que publicar la documentación que considere de uso confidencial.
- La EC distribuirá a todos los suscriptores y usuarios los términos y condiciones de uso.
- La EC dispondrá de un responsable de alto nivel con autoridad para aprobar la Declaración de Prácticas.

- La autoridad responsable de la Declaración de Prácticas se asegurará que estas están implantadas de forma correcta.
- La EC comunicará los cambios que llegue a realizar en la Declaración de Prácticas, estas deberán ser aprobadas y puestas a disposición de suscriptores y usuarios.

2.6.2 Declaración Informativa

La EC informará a todos los suscriptores y potenciales usuarios, los términos y condiciones sobre el uso de los certificados digitales.

Esta Declaración al menos especificará por cada política distinta utilizada:

- Contacto de la ER.
- Política de Registro aplicada.
- Al menos, un algoritmo resumen que se utilizará para representar a los datos.
- Cualquier limitación en el uso del servicio.
- Las obligaciones del suscriptor.
- Las obligaciones de los usuarios.
- Información de cómo verificar la validez de un certificado digital de forma que un usuario pueda considerar razonable confiar en él y cualquier posible limitación en la validez de este.
- El periodo de tiempo de retención de los ficheros de auditoría.
- El marco jurídico aplicable, incluido cualquier declaración de cumplimiento de las regulaciones jurídicas nacionales.
- Limitaciones de responsabilidad.
- Proceso de resolución de disputas.
- Si la ER ha sido auditada por un organismo independiente respecto a la conformidad con estas prácticas.
- Disponibilidad del servicio y expectativas de resolución ante incidentes que afecten a la emisión de certificados digitales.

2.7. Publicación y repositorios

2.7.1 Publicación de información de la AC

De manera general Camerfirma publica las siguientes informaciones en su repositorio:

- Un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida, o extinguida.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La política general de certificación y, cuando sea conveniente, las políticas específicas.
- Los perfiles de los certificados y de las listas de revocación de los certificados.
- La Declaración de Prácticas de Certificación y las PDS correspondientes (PKI Disclosure Statement).
- Los instrumentos jurídicos vinculantes con firmantes y verificadores.

Todo cambio en las especificaciones o condiciones del servicio será comunicado a los usuarios por la Entidad de Certificación, a través de su página web <http://www.camerfirma.com>

AC Camerfirma no retirará la versión anterior del documento objeto del cambio, indicando que ha sido sustituido por la versión nueva.

La publicación de certificados por AC subordinadas externas se realizan en un repositorio proporcionado por AC Camerfirma, o en su caso, en un repositorio propio al cual, por acuerdo contractual, Camerfirma puede tener acceso.

2.7.2 Frecuencia de publicación

AC Camerfirma publica los certificados de entidad final inmediatamente después de haber

sido emitidos y siempre tras la aprobación del Sujeto/Firmante.

AC Camerfirma emite y publica listas de revocados de forma periódica siguiendo la tabla marcada en el apartado correspondiente de estas prácticas de certificación: "Frecuencia de emisión de CRLs".

Camerfirma publica de forma inmediata en su página Web <https://policy.camerfirma.com>. Cualquier modificación en las Políticas y la CPS, manteniendo un histórico de versiones.

AC Camerfirma podrá retirar la referencia al cambio de la página principal al cabo de 15 (quince) días desde la publicación de la nueva versión y se insertaría en el depósito correspondiente. Las versiones antiguas de la documentación son conservadas al menos por un periodo de 15 (quince) años, pudiendo ser consultadas, con causa razonada por los interesados.

2.7.3 Controles de acceso a los repositorios

Camerfirma publica los certificados y CRLs en su página web. Para el acceso al directorio de certificados se necesitará el email del titular y pasar un control anti robot, eliminando así la posibilidad de búsquedas y descargas masivas.

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

Camerfirma utiliza sistemas fiables para el repositorio, de tal manera que:

- Se pueda comprobar la autenticidad de los certificados. El propio certificado mediante la firma por la autoridad de certificación garantiza su autenticidad.
- Las personas no autorizadas no puedan alterar los datos. La firma electrónica de la autoridad de certificación, protege de la manipulación de los datos incluidos en el certificado.
- El solicitante autoriza o no a la publicación de su certificado en el proceso de solicitud.

2.8. Auditorías

2.8.1 Frecuencia de las auditorías

Camerfirma España es una empresa comprometida con la seguridad y la calidad de sus servicios.

Los objetivos de Camerfirma España, como proveedor de operaciones de Camerfirma Perú, respecto a la seguridad y la calidad han sido fundamentalmente la obtención de la certificación ISO/IEC 27001, ISO/IEC 20000 y la realización de Auditorías internas bienales al Sistema de certificación Camerfirma, y fundamentalmente a las Autoridades de registro, para garantizar el cumplimiento de los procedimientos internos.

Camerfirma España está sujeta a unas auditorías periódicas con el sello WEBTRUST for CA, WEBTRUST SSL BR y WEBTRUST SSL EV que asegura que los documentos de políticas y CPS tienen un formato y alcance adecuado a la vez que están completamente alineadas con su políticas y prácticas de certificación.

Para la adecuación de conformidad eIDAS, AC Camerfirma realiza una evaluación de conformidad bienal tal como marca el reglamento de las siguientes normas: EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 421.

Camerfirma España está sujeta a una auditoría bienal sobre LOPD.

Camerfirma España realiza una auditoría interna a aquellas entidades que hayan obtenido un certificado de AC subordinada o TSU y que emitan y gestionen certificados con sus propios recursos técnicos y operativos. En esta auditoría Camerfirma comprueba de forma aleatoria un número de certificados emitidos por dicha autoridad de registro, asegurándose de que las evidencias recogidas sean correctas y suficientes para la emisión del certificado.

En calidad de Entidad de Registro, Camerfirma Perú se somete a evaluaciones técnicas del INDECOPI, las cuales deberán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.

2.8.2 Identificación y cualificación del auditor

La selección de los auditores depende del INDECOPI.

2.8.3 Relación entre el auditor y la ER

Los auditores o asesores deben ser independientes de la ER de Camerfirma Perú.

2.9. Confidencialidad

2.9.1 Tipo de información a mantener confidencial

Camerfirma España, como proveedor de operaciones de Camerfirma Perú, considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que la haya otorgado el carácter confidencial a dicha información, a no ser que exista una imposición legal.

Camerfirma España dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo de confidencialidad que deberán firmar todas las personas que tengan acceso a información confidencial.

Documentación de referencia: IN-2005-02-04-Política de Seguridad.

IN-2006-02-03-Normativa Seguridad.

Camerfirma cumple en todo caso con la normativa vigente en cada momento en materia de protección de datos. En este sentido, este documento sirve, de

conformidad con la Ley 59/2003, de Firma Electrónica (artículo 19.3) como documento de seguridad.

Documentación de referencia:

IN-2006-05-11-Conformidad de Requerimientos legales

2.9.2 Tipo de información considerada no confidencial

Se considerará como información no confidencial:

- a) La contenida en la presente Política y en las Prácticas de Certificación
- b) La información contenida en los certificados.
- c) Cualquier información cuya publicidad sea impuesta normativamente

2.9.3 Divulgación de información de revocación de certificados

Camerfirma España, como proveedor de operaciones de Camerfirma Perú, difunde la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRLs.

Camerfirma España dispone de un servicio de consulta de CRL y Certificados en el sitio de Internet: <http://www.camerfirma.com/area-de-usuario/consulta-de-certificados/>

Camerfirma España dispone de un servicio de consulta online de estado de los certificados basado en el estándar OCSP en la dirección <http://ocsp.camerfirma.com>. El servicio OCSP ofrece respuestas estandarizadas bajo el RFC 2560 sobre el estado de un certificado digital, es decir, si el certificado consultado está activo, revocado o si ha sido emitido o no por la autoridad de certificación.

La política de difusión de información de revocación de certificados en AC subordinadas Externas con uso de tecnología propia, se realizará en base a sus propias CPS.

2.9.4 Envío a la Autoridad Competente

Camerfirma España proporcionará la información solicitada por la autoridad competente o al organismo regulador correspondiente, en los casos y forma establecidos en la legislación vigente.

2.10. Derechos de propiedad intelectual

Camerfirma España y la ER de Camerfirma Perú tienen derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

3. Especificación de la Administración

3.1. Autoridad de las políticas

El departamento jurídico constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas.

3.2. Procedimientos de especificación de cambios

Cualquier elemento de esta política es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la Web de Camerfirma.

En la Web de Camerfirma se mantendrá un histórico con las versiones anteriores de las políticas.

Los usuarios afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

Si un cambio en la política afecta de manera relevante a un número significativo de usuarios de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

3.3. Procedimientos de aprobación de la DPC

Para la aprobación y autorización de una ER se deberán respetar los procedimientos especificados por la PA. Las partes de la DPC de una ER que contenga información relevante en relación a su seguridad, toda o parte de esa DPC no estará disponible públicamente.

4. Solicitud de Emisión de certificados digitales

4.1. Solicitud de certificados a persona jurídica

4.1.1 Servicios brindados

La ER de Camerfirma Perú brinda los siguientes servicios a personas jurídicas:

- a) Atención de solicitudes de emisión, revocación y re-emisión¹ de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
- b) Atención de solicitudes de emisión, revocación y re-emisión² de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
- c) Atención de solicitudes de emisión, revocación y re-emisión³ de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- d) Atención de solicitudes de emisión, revocación y re-emisión⁴ de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados brindados por la ER de Camerfirma Perú corresponden a las Entidades de Certificación acreditadas ante el INDECOPI que se encuentran publicadas en la siguiente dirección: www.camerfirma.com

4.1.2 Autorizadas para realizar la solicitud

Aquellas que puedan sustentar su existencia y vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos. Las personas jurídicas asumen la responsabilidad de titulares de los certificados digitales que adquieren. En este caso existen dos tipos de suscriptores: el representante legal y los funcionarios o empleados que por el cargo ocupan deben adquirir un certificado digital. En el certificado digital del representante legal quedarán registrados sus atributos o facultades, los cuales le permitirán utilizar el certificado digital para realizar transacciones en nombre y representación de la persona jurídica. Por otro lado, los certificados digitales de los funcionarios o empleados tienen atributos limitados al desenvolvimiento de sus funciones dentro de la persona jurídica.

Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad de certificados y de las

¹ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

² La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

³ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

⁴ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado.

4.1.3 Modalidades de atención

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante un contrato de adquisición de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de la ER de Camerfirma Perú
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER
- De realizarse de manera remota, deberá realizarse mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER de Camerfirma Perú, utilizando un certificado digital reconocido por el INDECOPI.

4.1.4 Solicitud de certificados de atributos

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

4.1.5 Solicitud de certificados para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

4.1.6 Reconocimiento, autenticación y rol de las marcas registradas

Conforme con la Guía de Acreditación de ER del INDECOPI, en el caso de personas jurídicas, la ER de Camerfirma Perú no asignará un nombre de titular

que haya sido ya asignado a un titular diferente. La ER de Camerfirma Perú se reserva el derecho de rechazar una solicitud de emisión de certificado digital a causa de un conflicto de nombres.

Por otro lado, no le corresponde a la ER de Camerfirma Perú determinar si al solicitante de un certificado digital le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado digital. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

4.1.7 Identificación y autenticación de solicitantes de certificados de persona jurídica

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información proporcionada por los solicitantes será validada a través de la consulta a la Superintendencia Nacional de los Registros Públicos.

En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

4.1.8 Contrato del titular

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato, que en adelante llamaremos "contrato del titular".

A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

4.1.9 Verificación de suscriptores

Los aspirantes a suscriptores deben ser validados en cualquiera de las siguientes modalidades:

- De manera presencial en las instalaciones de Camerfirma Perú en calidad de ER
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER

El proceso de verificación de sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER debe requerir a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo. Además, debe presentar el original de su propio documento oficial de identidad.

4.2. Solicitud de certificados de persona natural

4.2.1 Servicios brindados

La ER de Camerfirma Perú brinda los siguientes servicios a personas naturales:

- a) Atención de solicitudes de emisión, revocación y re-emisión⁵ de certificados para personas naturales de nacionalidad peruana.
- b) Atención de solicitudes de emisión, revocación y re-emisión ⁶ de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a la Entidad de Certificación de Camerfirma Perú, que se encuentran publicados en la siguiente dirección: www.camerfirma.com

4.2.2 Autorizados para realizar la solicitud

Aquellas que tienen plena capacidad de ejercicio de sus derechos civiles. Las personas naturales asumirán la responsabilidad de titulares y suscriptores de los certificados digitales que adquieren.

4.2.3 Modalidades de atención

La solicitud puede ser realizada mediante un contrato de adquisición de los certificados digitales que puede ser celebrado de las siguientes formas:

- De manera presencial en las instalaciones de la ER de Camerfirma Perú
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER de Camerfirma Perú, utilizando un certificado digital reconocido por el INDECOPI.

4.2.4 Solicitud de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento, portando el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento

4.2.5 Contrato del suscriptor

El solicitante deberá firmar un contrato, que en adelante llamaremos "contrato del suscriptor", el cual contiene las obligaciones que deben cumplir los

⁵ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

⁶ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

suscriptores y titulares de conformidad con la legislación de la materia para garantizar el efecto legal de las transacciones realizadas, establecidas por las ER de Camerfirma Perú, así como las consecuencias de no cumplir con el acuerdo.

Este contrato deberá ser firmado de manera digital o manuscrita por el solicitante, para luego ser archivado por la ER de Camerfirma Perú.

A través de dicho contrato, el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

4.2.6 Verificación de suscriptores

Los aspirantes a suscriptores deben ser validados en cualquiera de las siguientes modalidades:

- De manera presencial en las instalaciones de Camerfirma Perú en calidad de ER
 - De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER.

4.2.7 Identificación y autenticación de solicitantes de certificados de persona natural

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de Camerfirma Perú a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de Camerfirma Perú no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

5. Procesamiento de la solicitud

5.1. Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

- a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
- b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal

respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de Camerfirma Perú puede decidir establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

5.2. Aprobación de la solicitud de emisión de un certificado

En caso que una solicitud sea aprobada por la ER de Camerfirma Perú realizará lo siguiente:

- a) Comunicar a la EC su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC de Camerfirma Perú.
- b) Se requerirá la firma del contrato del suscriptor.

5.3. Registro de documentos

La ER de Camerfirma Perú registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

5.4. Método para probar la posesión de la clave privada

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor.

Los módulos criptográficos distribuidos por Camerfirma Perú cuentan con la certificación FIPS 140-2 o equivalente.

Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la respectiva EC en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

5.5. Tiempo para el procesamiento de la solicitud de un certificado

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de Camerfirma Perú enviará a la EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de cinco (05) días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

5.6. Emisión del certificado

La emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud. Dicho certificado tiene la vigencia de dos (02) años.

6. Solicitud de re-emisión de certificados digitales

La ER de Camerfirma Perú recibe solicitudes de re-emisión rutinaria. La re-emisión rutinaria es un proceso programado, que puede ejecutarse cada vez que un nuevo par de claves debe ser emitido debido a que la fecha de expiración de un certificado digital es cercana y menor de un plazo máximo de un (01) año. Solamente los titulares de certificados digitales pueden solicitar la re-emisión por certificado digital.

Luego de la expiración de un certificado digital re-emitido, deberá seguirse el proceso de solicitud de emisión de un nuevo certificado digital.

6.1. Solicitud de re-emisión certificados de persona jurídica

6.1.1 Servicios brindados

La ER de Camerfirma Perú brinda los siguientes servicios a personas jurídicas:

- a) Atención de solicitudes de re-emisión⁷ de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
- b) Atención de solicitudes de re-emisión de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
- c) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- d) Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: www.camerfirma.com

6.1.2 Autorizados para realizar la solicitud

Solo los titulares de certificados pueden solicitar la re-emisión de certificados, por lo que en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de Camerfirma Perú, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

⁷ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

6.1.3 Modalidades de atención

Para ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de Camerfirma Perú
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER, el Operador de Registro
- De realizarse de manera remota, deberá realizarse mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER de Camerfirma Perú, utilizando un certificado digital reconocido por el INDECOPI.

6.1.4 Solicitud de re-emisión de certificados de atributos

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

6.1.5 Solicitud de re-emisión de certificados para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

En la solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

6.1.6 Identificación y autenticación de solicitantes de re-emisión de certificados de persona jurídica

La ER de Camerfirma Perú comprobará que la información del titular y del suscriptor contenida en la solicitud continúa siendo válida, respecto de la existencia de la persona jurídica en los Registros Públicos y de los suscriptores en la base de datos del RENIEC.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

En el caso de empresas constituidas en el extranjero, el solicitante deberá acreditar la continuidad de su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

En el caso de suscriptores extranjeros, estos tendrán que presentar al Operador de Registro, su documento oficial de identidad, pasaporte o carnet de extranjería.

6.2. Solicitud de re-emisión de certificados de persona natural

6.2.1 Servicios brindados

La ER de Camerfirma Perú brinda los siguientes servicios a personas naturales:

- c) Atención de solicitudes de re-emisión⁸ de certificados para personas naturales de nacionalidad peruana.
- d) Atención de solicitudes de re-emisión⁹ de certificados de atributos para personas naturales de nacionalidad extranjera.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: www.camerfirma.com

6.2.2 Autorizados para realizar la solicitud

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado.

6.2.3 Modalidades de atención

La solicitud puede ser realizada mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de Camerfirma Perú
- De manera presencial en un lugar asignado por el solicitante en presencia de un representante de la ER, el Operador de Registro
- De realizarse de manera remota, deberá realizarse mediante un documento o correo electrónico firmado digitalmente

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER de Camerfirma Perú, utilizando un certificado digital reconocido por el INDECOPI.

6.2.4 Solicitud de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

6.2.5 Identificación y autenticación de solicitantes de certificados de persona natural

La información proporcionada por los solicitantes de nacionalidad peruana será validada por la ER de Camerfirma Perú a través de un mecanismo de consulta a las bases de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.

De manera general, no se incluirá en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción

⁸ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

⁹ La re-emisión dependerá de lo establecido en la Política de Certificación de la EC de Camerfirma Perú.

en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de Camerfirma Perú no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar documentos que respalden dichas modificaciones.

7. Procesamiento de la solicitud de re-emisión

7.1. Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

- a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
- b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de Camerfirma Perú puede decidir establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

7.2. Aprobación de la solicitud de emisión de un certificado

En caso que una solicitud sea aprobada por la ER de Camerfirma Perú realizará lo siguiente:

- a) Comunicar a la EC su aprobación para la re-emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC.
- b) Se requerirá la firma del contrato del suscriptor.

7.3. Registro de documentos

La ER de Camerfirma Perú registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

7.4. Método para probar la posesión de la clave privada

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor, en un módulo criptográfico con la certificación FIPS 140-2. Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la EC de Camerfirma Perú en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada.

7.5. Tiempo para el procesamiento de la solicitud de un certificado

Una vez validada la identidad del solicitante, si el resultado de la validación es positivo, la ER de Camerfirma Perú enviará a la EC la autorización de la emisión del certificado de manera inmediata.

El máximo tiempo de respuesta para la emisión del certificado será de cinco (05) días, luego de haber sido aprobada la validación de identidad y del pago respectivo.

7.6. Re-emisión del certificado

La re-emisión del certificado será realizada mediante el correo electrónico del suscriptor, registrado en su solicitud.

8. Solicitud de revocación de certificados

8.1. Circunstancias para realizar la solicitud

El titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE a través de lo estipulado en el contrato del suscriptor y/o titular.
- Por decisión de la legislación respectiva.

8.2. Solicitud de revocación de certificados

8.2.1 Servicios brindados

La ER de Camerfirma Perú brinda los siguientes servicios a personas jurídicas y naturales:

- a) Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.
- b) Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.
- c) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad peruana, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
- d) Atención de solicitudes de revocación de certificados de atributos para personas jurídicas de nacionalidad extranjera, para ser usados por funcionarios y personal específico, incluso por el Representante legal.
- e) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad peruana como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- f) Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas de nacionalidad extranjera como, por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados corresponden a las Entidades de Certificación acreditadas que se encuentran publicadas en la siguiente dirección: www.camerfirma.com

8.2.2 Autorizados para realizar la solicitud

De acuerdo a lo estipulado por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son:

- El titular del certificado
- El suscriptor del certificado.
- La EC o ER que emitió el certificado.
- Un juez que de acuerdo a la Ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento.

En el caso de personas jurídicas, los titulares de certificados pueden solicitar la re-emisión de certificados, por lo que en ambos casos, tanto certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER de Camerfirma Perú, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

8.2.3 Identificación y autenticación de los solicitantes

En los casos de que la solicitud sea presencial:

- Los suscriptores deben presentar en la ER como mínimo su documento oficial de identidad.
- El representante asignado por la persona jurídica debe presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.

- Los terceros (diferentes de la EC, el suscriptor y el titular) deberán presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo a la ley vigente, junto a la orden judicial respectiva

8.2.4 Modalidades de atención

La solicitud puede ser realizada por los titulares y suscriptores mediante las siguientes formas:

- De manera presencial en las instalaciones de la ER de Camerfirma Perú
- De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER, el Operador de Registro
- De manera remota, mediante un documento o correo electrónico firmado digitalmente por el representante asignado por la persona jurídica o por el suscriptor. El certificado digital a emplear no debe ser el que se desea revocar.
- De manera remota en una comunicación directa con la EC, mediante un control de acceso o contraseña brindados al suscriptor en el momento de la solicitud de emisión del certificado.

Para todos los demás actores, diferentes a los suscriptores y titulares, la solicitud deberá ser De manera presencial en las instalaciones de la ER de Camerfirma Perú.

La EC no requerirá realizar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato o en caso sea necesario por revocación del certificado de la EC. La EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su Declaración de Prácticas de Certificación y se encuentren de acuerdo con la legislación vigente.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER de Camerfirma Perú, utilizando un certificado digital reconocido por el INDECOPI.

8.2.5 Solicitud de revocación de certificados de atributos

El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

8.2.6 Solicitud de revocación de certificados para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica dueña del dispositivo.

8.2.7 Solicitud de revocación de certificados de persona natural

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

9. Procesamiento de la solicitud de revocación

9.1. Rechazo de la solicitud de revocación emisión de un certificado

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

- a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
- b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

La EC de Camerfirma Perú puede decidir establecer en su Declaración de Prácticas de Certificación u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER.

9.2. Aprobación de la solicitud de revocación de un certificado

En caso que una solicitud sea aprobada por la ER de Camerfirma Perú realizará lo siguiente:

- a) Comunicar a la EC su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por la EC.
- b) Una copia de dicha solicitud firmada será enviada a la EC o almacenada en la ER de Camerfirma Perú.

9.3. Registro de documentos

La ER de Camerfirma Perú registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de la misma a la EC de Camerfirma Perú, sus suscriptores y los terceros que confían.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

9.4. *Tiempo para el procesamiento de la solicitud de revocación*

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de Camerfirma Perú enviará a la respectiva EC la autorización de la revocación del certificado de manera inmediata.

El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación de la EC de Camerfirma Perú.

9.5. *Revocación del certificado*

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

10. Gestión de la seguridad

Las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los servicios de registro son señaladas en la Política de Seguridad de la ER de Camerfirma Perú.

11. Gestión de Operaciones

11.1. *Módulo criptográfico*

La generación de claves de los suscriptores debe ser realizada en módulos criptográficos FIPS 140-2.

Los módulos criptográficos usados por los Operadores de Registro deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.

11.2. *Restricciones de la generación de claves*

Las claves pueden ser generadas solamente por los propios suscriptores.

11.3. *Entrega de la clave pública*

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ERs acepten las claves públicas en representación de los emisores de los certificados, estas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

11.4. *Depósito de clave privada*

La ER de Camerfirma Perú no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

11.5. Datos de activación

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de Camerfirma Perú, se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

12. Controles de seguridad computacional

Los sistemas de registro utilizados por Camerfirma Perú son provistos y administrados por EC reconocidas por el INDECOPI, con la certificación Webtrust. La ER sólo accede a estos sistemas vía web con acceso vía certificados digitales de los Operadores de Registro.

13. Materias de negocio y legales

13.1. Tarifas

Las tarifas por los servicios de registro y certificación digital se indican en la sección 2.5. *Tarifas*.

13.2. Políticas de reembolso

Las políticas de reembolso por los servicios los servicios de registro serán definidas en los contratos de titulares.

13.3. Cobertura de seguro

Camerfirma Perú proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil de la Entidad de Certificación.

13.4. Provisiones y garantías

Las garantías por los servicios de registro y certificación digital serán definidas en los contratos de titulares, en relación a errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

13.5. Excepciones de garantías

La ER de Camerfirma Perú no se responsabiliza en casos de compromiso de la clave en manos del suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento.

13.6. Obligaciones de los suscriptores y titulares

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.

En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación de sus certificados en casos de compromiso de su clave privada.

13.7. Obligaciones de los terceros que confían

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

13.8. Indemnización

Los casos de indemnización son definidos en los contratos de los titulares.

13.9. Notificaciones

Los medios de notificación serán definidos en los contratos de titulares y suscriptores.

13.10. Enmendaduras y cambios

Las enmendaduras y cambios serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

13.11. Resolución de disputas

El procedimiento de resolución de disputas será definido en los contratos de los titulares.

13.12. Conformidad con la Ley aplicable

La ER de Camerfirma Perú se compromete a cumplir la ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

13.13. Subrogación

La ER de Camerfirma Perú no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes son especificados en este documento.

13.14. Fuerza mayor

Las cláusulas de fuerza mayor serán definidas en los contratos de los titulares.

14. Cumplimiento de requerimientos legales

Camerfirma Perú, como Autoridad emisora de sellos de tiempo, cumple los requerimientos legales establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales – Ley 27269.

15. Conformidad

Este documento ha sido aprobado por la Autoridad de la ER de Camerfirma Perú, y tiene carácter normativo sobre todos los servicios de sellado de tiempo, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

Anexo I. Acrónimos

AC	Autoridad de Certificación
AR	Autoridad de Registro
CPS	<i>Certification Practice Statement</i> . Declaración de Prácticas de Certificación
CRL	<i>Certificate Revocation List</i> . Lista de certificados revocados
CSR	<i>Certificate Signing Request</i> . Petición de firma de certificado
DES	<i>Data Encryption Standard</i> . Estándar de cifrado de datos
DN	<i>Distinguished Name</i> . Nombre distintivo dentro del certificado digital
DSA	<i>Digital Signature Algorithm</i> . Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
DSADCF	Dispositivo seguro de almacén de datos de creación de firma
FIPS	<i>Federal Information Processing Standard Publication</i>
IETF	<i>Internet Engineering Task Force</i>
ISO	<i>International Organization for Standardization</i> . Organismo Internacional de Estandarización
ITU	<i>International Telecommunications Union</i> . Unión Internacional de Telecomunicaciones
LDAP	<i>Lightweight Directory Access Protocol</i> . Protocolo de acceso a directorios
OCSP	<i>On-line Certificate Status Protocol</i> . Protocolo de acceso al estado de los certificados
OID	<i>Object Identifier</i> . Identificador de objeto
PA	<i>Policy Authority</i> . Autoridad de Políticas
PC	Política de Certificación
PIN	<i>Personal Identification Number</i> . Número de identificación personal
PKI	<i>Public Key Infrastructure</i> . Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA-1	<i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash
SSL	<i>Secure Sockets Layer</i> . Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	<i>Transmission Control Protocol/Internet Protocol</i> . Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

Anexo II. Definiciones

Autoridad de Certificación	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y la Parte Usaria, vinculando una determinada clave pública con una persona.
Autoridad de políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y DPC.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	El establecimiento de una relación de confianza entre dos AC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma .
Clave privada	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma . La clave privada de la AC será usada para firma de certificados y firma de CRL's
CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DSADCF	<i>Dispositivo seguro de almacén de los datos de creación de firma.</i> Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.

DSCF	<i>Dispositivo Seguro de creación de firma.</i> Elemento software o hardware empleado por el suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
Entidad	Dentro del contexto de las políticas de certificación de Camerfirma, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el suscriptor.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: <ul style="list-style-type: none"> a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes
Suscriptor	Dentro del contexto de las políticas de certificación de Camerfirma, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Parte Usuaría	Dentro del contexto de las políticas de certificación de Camerfirma, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado