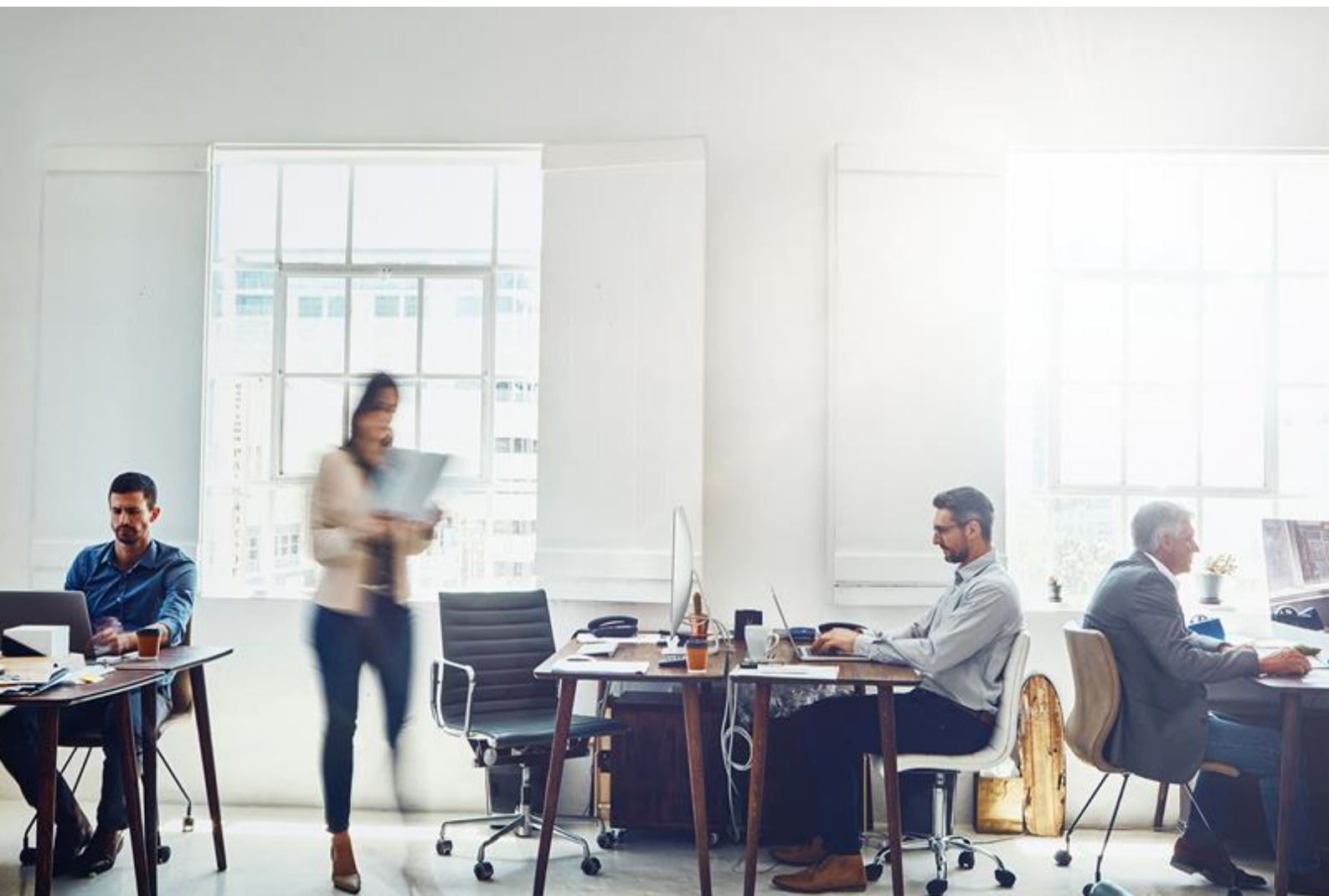


Política de Certificación

Certificados de firma electrónica

Versión: 240123

Clasificación: Público



Histórico de versiones

Versión	Sección y cambios	Fecha de Publicación
190121	<ul style="list-style-type: none"> Nueva Política de Certificación de Certificado personales que agrupa las diferentes políticas que existían sobre este tipo de certificados, que pueden ser consultadas en http://firmaprofesional.com/cps 	21/01/2019
190507	<ul style="list-style-type: none"> Se añade la comprobación del correo electrónico del solicitante previa a la emisión del certificado. Reestructurados los OIDs, eliminando duplicidades. Corrección de errores. Cambio de la CA que emite los certificados de Empleado Público a "AC Firmaprofesional - CUALIFICADOS". 	07/05/2019
200417	<ul style="list-style-type: none"> Incorporación de medidas por Estado de Alarma del COVID-19 Se añade la posibilidad de emitir los "Certificados Personales. En DCCF centralizado / 1.3.6.1.4.1.13177.10.1.40.3" 	17/04/2020
210217	<ul style="list-style-type: none"> Adaptación a la nueva Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza. 	17/02/2021
220216	<ul style="list-style-type: none"> Adaptación a la RFC 3647 Incorporación referencia Certificados de seudónimo como certificados con número de identificación profesional conforme al RD 203/2021 	16/02/2022
220510	<ul style="list-style-type: none"> Incorporación OID 1.3.6.1.4.1.13177.10.1.14 Actualización apartado 1.4.1.1 	10/05/2022
230616	<ul style="list-style-type: none"> Actualización apartado 1.4.1.1 limitación 3 años certificados emitidos en QSCD tarjeta o token Actualización apartado 1.3.1 Actualización apartado 3.1 	16/06/2023
230828	<ul style="list-style-type: none"> Modificación del apartado 1.4.1 Usos apropiados de los certificados: aclaraciones sobre el uso de los certificados de firma electrónica con las Administraciones Públicas 	28/08/2023
240123	<ul style="list-style-type: none"> Modificación del apartado 1.4.1.1 para la eliminación de la validez a 4 años de los certificados de empleado público, que pasarán a ser de hasta 5 años 	23/01/2024

Índice

1. Introducción	13
1.1. Resumen	13
1.2. Identificación del Documento	15
1.3. Entidades participantes	17
1.3.1 Autoridades de Certificación (CA)	17
1.3.2 Autoridad de Registro (RA)	17
1.3.3 Suscriptores	18
1.3.3.1 Solicitante	18
1.3.3.2 Firmante	19
1.3.4 Terceros que confían en los certificados	19
1.3.5 Otros participantes	20
1.4 Uso de los certificados	21
1.4.1 Usos apropiados de los certificados	21
1.4.1.1 Periodo de validez de los certificados.....	21
1.4.1.2 Dispositivos Cualificados de Creación de Firma	22
1.4.2 Usos prohibidos de los certificados	22
1.5 Administración de Políticas	23
1.5.1 Organización que administra el documento	23
1.5.2 Persona de contacto	23
1.5.3 Persona que determina la idoneidad de la CP para la póliza	23
1.5.4 Procedimiento de aprobación de la CP.....	23
1.6 Definiciones y siglas	23
2. Repositorios y Publicación de la Información	24
2.1 Repositorios.....	24
2.2 Publicación de información de certificación.....	24

2.3 Hora o frecuencia de publicación	24
2.4 Control de acceso a los repositorios.....	24
3. Identificación y Autenticación	25
3.1 Registro de Nombres	25
3.1.1 Tipos de nombres.....	25
3.1.2 Necesidad de que los nombres sean significativos.....	25
3.1.3 Anonimato o seudónimo de los suscriptores	25
3.1.4 Reglas para interpretar varias formas de nombres.....	25
3.1.5 Unicidad de los nombres	26
3.1.6 Reconocimiento, autenticación y función de las marcas	26
3.2 Validación inicial de la identidad	26
3.2.1 Método de prueba de posesión de clave privada.....	26
3.2.2 Autenticación de la identidad de la organización e identidad de dominio	26
3.2.3 Autenticación de la identidad de una persona física	26
3.2.4 Información de suscriptor no verificada.....	26
3.2.5 Validación de la identidad de la RA y de operadores de la RA.....	26
3.2.6 Criterios de interoperabilidad	27
3.3 Identificación y autenticación para solicitudes de renovación de claves	27
3.3.1 Identificación y autenticación para el cambio de clave	27
3.3.2 Identificación y autenticación para la renovación de certificados tras su revocación	27
3.4 Identificación y autenticación para solicitud de revocación	27
4. Requisitos operativos del ciclo de vida del certificado	27
4.1. Solicitud del certificado	27
4.1.1 Quién puede enviar una solicitud de certificado.....	27
4.1.2 Proceso de solicitud de certificados y responsabilidades	28
4.2 Tramitación de las solicitudes de certificados.....	28
4.2.1 Realización de las funciones de identificación y autenticación.....	28
4.2.2 Aprobación o denegación de las solicitudes de certificados.....	28
4.2.3 Tiempo de tramitación de las solicitudes de certificado.....	30

4.3 Emisión de certificados	30
4.3.1 Acciones de la CA durante la emisión del certificado	30
4.3.2 Notificación al suscriptor por parte de la CA de la emisión del certificado y entrega	32
4.4 Aceptación del certificado	32
4.4.1 Forma en la que se acepta el certificado	32
4.4.2 Publicación del certificado por la CA	33
4.4.3 Notificación de la emisión del certificado por parte de la CA a otras entidades	33
4.5 Uso de la claves y del certificado	33
4.5.1 Uso de certificado y clave privada del suscriptor	33
4.5.2 Uso de certificados y claves públicas de parte que confía	33
4.6 Renovación del certificado (sin cambio de claves)	33
4.6.1 Circunstancia para la renovación del certificado	33
4.6.2 Quién puede solicitar la renovación	34
4.6.3 Procesamiento de solicitudes de renovación de certificados	34
4.6.4 Notificación al suscriptor de la emisión de un nuevo certificado	35
4.6.5 Conducta que constituye la aceptación de un certificado de renovación	35
4.6.6 Publicación del certificado de renovación por parte de la CA	35
4.6.7 Notificación de la emisión del certificado por parte de la CA a otras entidades	35
4.7 Renovación del certificado con cambio de clave	35
4.7.1 Circunstancia para el cambio de clave del certificado	35
4.7.2 Quién puede solicitar la certificación de una nueva clave pública	36
4.7.3 Procesamiento de solicitudes de cambio de claves de certificados	36
4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado	37
4.7.5 Conducta que constituye la aceptación de un certificado con clave nueva	37
4.7.6 Publicación del certificado con nueva clave por parte de la CA	37
4.8 Modificación del certificado	37
4.8.1 Circunstancia para la modificación del certificado	37
4.8.2 Quién puede solicitar la modificación del certificado	37
4.8.3 Procesamiento de solicitudes de modificación de certificados	38

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado	38
4.8.5 Conducta que constituye la aceptación del certificado modificado	38
4.8.6 Publicación del certificado modificado por la CA	38
4.8.7 Notificación de la emisión del certificado por parte de la CA a otras entidades....	38
4.9 Revocación y suspensión de certificados.....	39
4.9.1 Circunstancias para la revocación.....	39
4.9.2 Quién puede solicitar la revocación	39
4.9.3 Procedimiento de solicitud de revocación	39
4.9.4 Periodo de gracia de la solicitud de revocación	39
4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación.....	39
4.9.6 Requisito de verificación de revocación para las partes que confían	40
4.9.7 Frecuencia de emisión de CRL.....	40
4.9.8 Latencia máxima para las CRL.....	40
4.9.9 Disponibilidad de verificación de estado / revocación en línea	40
4.9.10 Requisitos de verificación de revocación en línea.....	40
4.9.11 Otras formas de anuncios de revocación disponibles.....	40
4.9.12 Requisitos especiales relacionados con el compromiso clave.....	41
4.9.13 Circunstancias para la suspensión	41
4.9.14 Quién puede solicitar la suspensión.....	41
4.9.15 Procedimiento de solicitud de suspensión	41
4.9.16 Límites del período de suspensión	41
4.10 Servicios de estado de certificados.....	42
4.10.1 Características operativas	42
4.10.2 Disponibilidad del servicio	42
4.10.3 Funciones opcionales	42
4.11 Finalización de la suscripción.....	42
4.12 Custodia y recuperación de claves	42
4.12.1 Política y prácticas de custodia y recuperación de claves.....	43
4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión	43

5.1 Controles físicos.....	45
5.1.1 Ubicación y construcción del sitio	45
5.1.2 Acceso físico	45
5.1.3 Energía y aire acondicionado	45
5.1.4 Exposición al agua	45
5.1.5 Prevención y protección contra incendios	46
5.1.6 Almacenamiento de medios.....	46
5.1.7 Eliminación de residuos.....	46
5.1.8 Respaldo fuera de las instalaciones	46
5.2 Controles de procedimiento.....	46
5.2.1 Roles de confianza	46
5.2.2 Número de personas necesarias por tarea	47
5.2.3 Identificación y autenticación para cada rol.....	47
5.2.4 Roles que requieren separación de funciones.....	47
5.3 Controles de personal.....	47
5.3.1 Calificaciones, experiencia y requisitos de autorización.....	47
5.3.2 Procedimientos de verificación de antecedentes.....	47
5.3.3 Requisitos de formación	48
5.3.4 Frecuencia y requisitos de reentrenamiento	48
5.3.5 Frecuencia y secuencia de la rotación del trabajo.....	48
5.3.6 Sanciones por acciones no autorizadas	48
5.3.7 Requisitos de los contratistas independientes	48
5.3.8 Documentación suministrada al personal	48
5.4 Procedimientos de registro de auditorías.....	49
5.4.1 Tipos de eventos registrados	49
5.4.2 Frecuencia de procesado de registros de auditoría.....	49
5.4.3 Período de conservación del registros de auditoría.....	49
5.4.4 Protección de los registros de auditoría	49
5.4.5 Procedimientos de respaldo de los registros de auditoría.....	49

5.4.6 Sistema de recogida de auditorías	50
5.4.7 Notificación al sujeto causante del evento	50
5.4.8 Análisis de vulnerabilidades	50
5.5 Archivo de registros	50
5.5.1 Tipos de registros archivados	50
5.5.2 Período de conservación del archivo	50
5.5.3 Protección del archivo	51
5.5.4 Procedimientos de copia de seguridad del archivo	51
5.5.5 Requisitos para el sellado de tiempo de los registros	51
5.5.6 Sistema de recogida de archivos	51
5.5.7 Procedimientos para obtener y verificar la información del archivo	51
5.6 Cambio de claves	51
5.7 Plan de recuperación de desastres	52
5.7.1 Procedimientos de gestión de incidentes y compromisos	52
5.7.2 Los recursos informáticos, el software y/o los datos se corrompen	52
5.7.3 Procedimientos de compromiso de la clave privada de la entidad	52
5.7.4 Capacidades de continuidad del negocio después de un desastre	52
5.8 Cese de la actividad de la RA o CA	52
6. Controles de seguridad técnica	53
6.1 Generación e instalación del par de claves	53
6.1.1 Generación del par de claves	53
6.1.2 Entrega de la clave privada al suscriptor	53
6.1.4 Entrega de la clave pública de la CA a las partes confiantes	53
6.1.5 Tamaño de las claves	53
6.1.6 Generación de parámetros de clave pública y control de calidad	54
6.1.7 Propósitos de uso de la clave (según el campo de uso de la clave X.509 v3)	54
6.2 Protección de la clave privada y controles de ingeniería del módulo criptográfico	54
6.2.1 Normas y controles del módulo criptográfico	54
6.2.2 Control multipersona (k de n) de la clave privada	54

6.2.3 Depósito de claves privadas	54
6.2.4 Copia de seguridad de la clave privada	54
6.2.5 Archivo de claves privadas.....	55
6.2.6 Transferencia de claves privadas hacia o desde un módulo criptográfico	55
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico	55
6.2.8 Método de activación de la clave privada.....	55
6.2.9 Método de desactivación de la clave privada	55
6.2.10 Método de destrucción de la clave privada.....	55
6.2.11 Clasificación del módulo criptográfico.....	55
6.3 Otros aspectos de la gestión de pares de claves	56
6.3.1 Archivo de la clave pública.....	56
6.3.2 Periodos de funcionamiento del certificado y períodos de uso del par de claves..	56
6.4 Datos de activación.....	56
6.4.1 Generación e instalación de datos de activación	56
6.4.2 Protección de los datos de activación	56
6.4.3 Otros aspectos de los datos de activación	57
6.5 Controles de seguridad informática	57
6.5.1 Requisitos técnicos específicos de seguridad informática	57
6.5.2 Evaluación de la seguridad informática	57
6.6 Controles técnicos del ciclo de vida	57
6.6.1 Controles de desarrollo del sistema	57
6.6.2 Controles de gestión de la seguridad	57
6.6.3 Controles de seguridad del ciclo de vida	57
6.7 Controles de seguridad de la red	58
6.8 Control de tiempo	58
7. Perfiles de los certificados , CRL y OCSP.....	58
7.1 Perfil del certificado	58
7.1.1 Número(s) de versión	58
7.1.2 Extensiones del certificado.....	58

7.1.3	Identificadores de objetos de algoritmos	58
7.1.4	Formas del nombre	59
7.1.5	Restricciones del nombre	59
7.1.6	Identificador del objeto de la política del certificado	59
7.1.7	Uso de la extensión Policy Constraints	61
7.1.8	Sintaxis y semántica de los calificadores de política	61
7.1.9	Semántica de procesamiento de la extensión critical Certificate Policies.....	62
7.2	Perfil CRL.....	62
7.2.1	Número(s) de versión	62
7.2.2	Extensiones de CRL y entradas de CRL	62
7.3	Perfil OCSP	62
7.3.1	Número(s) de versión	62
7.3.2	Extensiones OCSP	62
8.	Auditorías de cumplimiento y otros controles	63
8.1	Frecuencia de las auditorías	63
8.2	Cualificación del auditor o evaluador	63
8.3	Relación entre el auditor y la autoridad auditada.....	63
8.4	Aspectos cubiertos por la evaluación.....	63
8.5	Acciones a emprender como resultado de la detección de deficiencias	63
9.	Otras cuestiones legales y de la actividad	64
9.1	Tarifas.....	64
9.1.1	Tarifas de emisión o renovación de certificados	64
9.1.2	Tarifas de acceso a los certificados.....	64
9.1.3	Tarifas de acceso a la información de revocación o de estado	64
9.1.4	Tarifas por otros servicios.....	64
9.1.5	Tarifas de reembolso	64
9.2	Responsabilidades económicas.....	65
9.2.1	Cobertura del seguro.....	66
9.2.2	Otros activos.....	66

9.2.3 Cobertura de seguro o garantía para las entidades finales	66
9.3 Confidencialidad de la información comercial	66
9.3.1 Alcance de la información confidencial	66
9.3.2 Información no confidencial.....	66
9.3.3 Responsabilidad de proteger la información confidencial.....	67
9.4 Protección de la información personal	67
9.4.1 Política de protección de datos de carácter personal	67
9.4.2 Información tratada como privada.....	67
9.4.3 Información no considerada privada	67
9.4.4 Responsabilidad de proteger la información privada	67
9.4.5 Aviso y consentimiento para el uso de la información privada.....	68
9.4.6 Divulgación en virtud de un proceso judicial o administrativo	68
9.4.7 Otras circunstancias de divulgación de información	68
9.5 Derechos de propiedad intelectual	68
9.6 Obligaciones y garantías.....	68
9.6.1 Obligaciones de la AC	68
9.6.2 Obligaciones de la AR	69
9.6.3 Obligaciones de los solicitantes	69
9.6.4 Representaciones y garantías de los terceros que confían en los certificados	69
9.6.5 Declaraciones y garantías de otros participantes.....	69
9.7 Exención de garantía.....	69
9.8 Limitaciones de responsabilidad	70
9.9 Indemnizaciones	70
9.10 Periodo de validez y terminación.....	70
9.10.1 Plazo	70
9.10.2 Terminación	70
9.10.3 Efecto de la terminación y supervivencia	70
9.11 Avisos y comunicaciones individuales con los participantes	71
9.12 Modificaciones o cambios en las especificaciones.....	71

9.12.1 Procedimiento para los cambios	71
9.12.2 Mecanismo y plazo de notificación	71
9.12.3 Circunstancias en las que debe modificarse la OID	71
9.13 Disposiciones para la resolución de conflictos	71
9.14 Normativa aplicable	72
9.15 Cumplimiento de la normativa aplicable	72
9.16 Disposiciones diversas	72
9.16.1 Acuerdo completo	72
9.16.2 Independencia	72
9.16.3 Resolución por vía judicial	72
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)	73
9.16.5 Fuerza mayor	73
9.17 Otras disposiciones	73

1. Introducción

1.1. Resumen

El certificado de firma electrónica, como lo define el Reglamento UE 910/2014, del Parlamento y del Consejo, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas (en adelante, "eIDAS"), es una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.

Los Certificados de firma electrónica contenidos en esta Política son certificados cualificados de persona física para firma electrónica según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en lo sucesivo, "Ley 6/2020 LSEC") y cumplen los requisitos establecidos en el anexo I del Reglamento eIDAS.

La solicitud y emisión de estos certificados se puede realizar a través de las Autoridades de Registro de FirmaProfesional habilitadas para tal fin.

La Autoridad de Registro puede ser diferente en función de cada Certificado. Esta Política de Certificación (en adelante, "Política" o "CP") está integrada por tres tipos de Certificados siendo las Autoridades de Registro las siguientes:

1. **Corporativos.** Diferenciados a su vez en:
 - a. de Colegiado -> La solicitud y emisión se realiza a través de los propios Colegios Profesionales a los que se vincula cada certificado, siendo obtenido por el colegiado.
 - b. de Persona Física -> La solicitud y emisión se realiza a través de las propias Corporaciones a las que se vincula cada certificado u otras entidades no vinculadas con el firmante que sean Autoridades de Registro de FirmaProfesional.
 - c. de Representación -> En estos tipos de certificado, la solicitud y emisión se realiza a través de las Autoridades de Registro de FirmaProfesional
 - i. Representante de entidad sin personalidad jurídica
 - ii. Representante legal
 - iii. Representante voluntario

2. **Personales** -> La solicitud y emisión también se realizará a través de las Autoridades de Registro de Firma Profesional habilitadas para tal fin.
3. **Empleado Público** -> Los certificados de Empleado Público son expedidos de conformidad con los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público para la firma electrónica del personal al servicio de las Administraciones Públicas y se adapta a las definiciones de los niveles de aseguramiento alto y medio y a los perfiles de certificados establecidos en el punto 10 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Se pueden distinguir dos tipos de certificados:

- a. Certificados de empleado público
- b. Certificados de empleado público con seudónimo.

En ambos tipos, la solicitud y emisión se realiza a través de la Administración Pública, que expide estos certificados a funcionarios, personal laboral, estatutario y personal autorizado, siempre en el ejercicio de sus funciones, permitiendo identificar telemáticamente a los suscriptores como Administraciones Públicas y a los firmantes como personas al servicio de la Administración Pública.

En el presente documento se exponen las condiciones particulares referentes a todos los certificados que integran esta Política de Certificación. A su vez, la Política de Certificación (en adelante, la "CP") está sujeta al cumplimiento de la Declaración de Prácticas de Certificación (en adelante, la "CPS") de Firmaprofesional, a la que incorpora por referencia.

1.2. Identificación del Documento

Nombre:	CP Certificados de Firma Electrónica
Versión:	230616
Descripción:	Política de Certificación para Certificados de Firma Electrónica, donde quedan agrupados los certificados emitidos a personas físicas con y sin atributos.
Fecha de Emisión:	16/06/2023
OIDs:	<p>1.3.6.1.4.1.13177.10.1.1.D (*) Certificados Corporativos de Colegiado</p> <p>1.3.6.1.4.1.13177.10.1.2.D (*) Certificados Corporativos de Persona Física</p> <p>1.3.6.1.4.1.13177.10.1.14. D (*) Certificados Corporativos de Persona Física con firma de correo</p> <p>1.3.6.1.4.1.13177.10.1.11.D (*) Certificados Corporativos de Representante Legal</p> <p>1.3.6.1.4.1.13177.10.1.12.D (*) Certificados Corporativos de Representante Voluntario frente a las Administraciones Públicas</p> <p>1.3.6.1.4.1.13177.10.1.13.D (*) Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica</p> <p>1.3.6.1.4.1.13177.10.1.22.D (*) Certificados de Empleado Público</p> <p>1.3.6.1.4.1.13177.10.1.23.D (*) Certificados de empleado público con seudónimo</p> <p>1.3.6.1.4.1.13177.10.1.40.D (*) Certificados Personales</p>
Localización:	http://www.firmaprofesional.com/cps

(*)D = Dispositivo / Nivel de Seguridad:

- 1 = DCCF portable (Nivel Alto)
- 2 = Otros dispositivos (Nivel Medio)
- 3 = DCCF centralizado

Esta Política de Certificación agrupa las siguientes Políticas, que quedan derogadas con la publicación de la versión 190121 de la presente:

- Política de Certificados Corporativos de Colegiado Versión 171121.
- Política de Certificados Corporativos de Persona Física. Versión 171121.

- Política de Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica Versión 180328.
- Política de Certificados Corporativos de Representante Legal Versión 171121.
- Política de Certificados Corporativos de Representante Voluntario frente a las Administraciones Públicas Versión 171121.
- Política de Certificados Personales Versión 171121.
- Política de Certificados de empleado público Versión 171121.

Todas estas Políticas derogadas pueden ser consultadas en <https://www.firmaprofesional.com/cps>, en el apartado "Políticas y Prácticas de Certificación anteriores"

1.3. Entidades participantes

1.3.1 Autoridades de Certificación (CA)

Todos los certificados de esta Política deben ser emitidos por FirmaProfesional como Prestador de Servicios de Confianza que emite certificados cualificados según la Ley 6/2020 y el Reglamento UE 910/2014 (eIDAS).

Los certificados corporativos, los certificados personales y los certificados de empleado público son emitidos por la Autoridad de Certificación (CA) Subordinada "AC Firmaprofesional - CUALIFICADOS" o "FIRMAPROFESIONAL ICA B01 QUALIFIED 2022".

1.3.2 Autoridad de Registro (RA)

La gestión de las solicitudes y las emisiones de los certificados será realizada por las entidades que actúen como Autoridades de Registro de Firmaprofesional.

Cada Autoridad de Registro establecerá:

- Los criterios que se deben cumplir para solicitar un certificado, sin entrar en contradicción con lo estipulado en la CPS y la presente CP.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del firmante, cumpliendo con lo estipulado en la CPS y en esta CP.
- Los dispositivos de creación de firma a utilizar, de entre los que previamente Firmaprofesional haya homologado.

La Corporación o Colegio Profesional que actúe como RA podrá delegar estas funciones a una entidad de confianza cuando la ubicación geográfica de los suscriptores (ver punto 2.4) represente un problema logístico para la identificación del solicitante en la solicitud y entrega de certificados. Para poder justificar esta delegación, la entidad de confianza debe tener una especial vinculación con la RA y una relación de proximidad con los solicitantes de los certificados.

La entidad de confianza deberá firmar un acuerdo de colaboración con la RA en el que se acepte la delegación de estas funciones. Firmaprofesional deberá autorizar de manera expresa y previa el modelo de acuerdo a firmar.

1.3.3 Suscriptores

El Suscriptor es la persona física o jurídica que ha contratado los servicios de confianza de Firmaprofesional y que, por lo tanto, será el propietario del certificado. En consecuencia, tendrá los derechos de revocación y suspensión sobre el certificado.

Dependiendo del tipo de Certificado, el Suscriptor puede ser:

- El Colegio Profesional en los Certificados de Colegiado.
- La Corporación en los Certificados Corporativos de Persona Física y en todo aquellos de Representantes (de Entidad sin Personalidad Jurídica, Legal y Voluntario frente Administraciones Públicas).
- El propio solicitante, en el caso de certificados personales
- La Administración, Órgano o Entidad de derecho público en los Certificados de Empleado Público y de Empleado Público con seudónimo.

1.3.3.1 Solicitante

Solicitante es la persona física mayor de edad que en nombre propio solicita la emisión de un certificado a Firmaprofesional.

Sin embargo, para determinados Certificados, la persona física necesitará estar dotada de una condición especial. Por ello, podrán solicitar los certificados, dependiendo de cada tipo:

- Los Certificados Corporativos de Colegiado:
 - Cualquier profesional colegiado en un colegio profesional.
 - El propio Colegio Profesional, en nombre y asistencia del colegiado.
- Los Certificados Corporativos de Persona Física:
 - El representante legal o voluntario de la Corporación, o una persona autorizada por él, en nombre de los empleados o personas vinculadas con la indicada Corporación.
 - Cualquier persona vinculada a una Corporación que actúe como RA de Firmaprofesional, según los criterios que establezca la propia Corporación.

- Los profesionales autónomos o empresarios individuales. En este caso, al no disponer de una personalidad jurídica que los represente, podrán solicitar un Certificado Corporativo de Persona Física en el que la identidad de la persona física y de la persona jurídica serán iguales.
- Los Certificados Corporativos de Representante sin Personalidad Jurídica:
 - Ser Representante de la Entidad sin Personalidad Jurídica suscriptora del certificado con poderes específicos generales para actuar ante las Administraciones Públicas.
- Los Certificados Corporativos de Represente Legal:
 - el administrador (único o solidario) o el apoderado con poderes generales.
- Los Certificados Corporativos de Representante Voluntario frente Administraciones Públicas:
 - Ser Representante voluntario de la Corporación suscriptora del certificado con poderes específicos generales para actuar ante las Administraciones Públicas.
- Los Certificados de Empleado Público y de Empleado Público con seudónimo:
 - Ser un empleado público que dependa de una Corporación Pública establecida como RA de FirmaProfesional.

1.3.3.2 Firmante

El firmante es la persona física que crea la firma electrónica. Para ello, esta persona física debe estar identificada por su nombre, apellidos y NIF, NIE o número de pasaporte, excepto en los Certificados de Empleado Público con seudónimo, que la persona física está identificada por un seudónimo.

1.3.4 Terceros que confían en los certificados

Los certificados recogidos en esta Política son certificados cualificados que cumplen los requisitos que establece la Ley 6/2020 y el Reglamento eIDAS.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso, tanto cuantitativas como cualitativas, contenidas en la CPS, en la presente CP y en el propio certificado.

Por último, todos los certificados emitidos bajo la presente Política están reconocidos por @firma, la Plataforma de validación y firma electrónica del Gobierno de España.

1.3.5 Otros participantes

Sin estipulación.

1.4 Uso de los certificados

1.4.1 Usos apropiados de los certificados

Los certificados emitidos por Firmaprofesional podrán usarse en los términos establecidos por la normativa vigente aplicable a la firma electrónica, con las condiciones adicionales que se establecen en la CPS y en esta CP.

Asimismo, los certificados emitidos bajo esta CP pueden ser utilizados con los siguientes propósitos:

- Garantizar la identidad del firmante.
- Garantizar la integridad del documento firmado.
- Identificar al firmante del documento. En el caso de los Certificados de Empleado Público con seudónimo la identificación será mediante seudónimo.

Se permite el uso de estos certificados en las relaciones del firmante con las Administraciones Públicas y en los usos estrictamente particulares. En el caso de los certificados de representante voluntario ante las Administraciones Públicas, se limita el uso a aquellos que le permitan los poderes de representación.

Para poder utilizar los certificados con la Administración pública es necesario que conste como parte de la identidad del titular el número del Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal español, En cualquier otro caso NO PODRÁN UTILIZARSE para la tramitación con la Administración Pública Española.

1.4.1.1 Periodo de validez de los certificados

El periodo de validez será el que se indique en el propio certificado. Este período tiene un plazo máximo de 5 años para todos los Certificados contenidos en esta Política.

Los certificados con extensión e-mail protection cuya CA Raíz esté en los navegadores, tendrán un período de validez máximo de 3 años.

Los certificados emitidos en QSCD tarjeta o Token tendrán una duración máxima de 3 años.

1.4.1.2 Dispositivos Cualificados de Creación de Firma

En los casos en que Firmaprofesional pueda garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Cualificado de Creación de Firma (DCCF), sea portable o centralizado, en cumplimiento de los requisitos establecidos en el Anexo II del Reglamento UE 910/2014 eIDAS, esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión "Certificate Policies" con valor OID de la política de certificación propia de Firmaprofesional correspondiente al certificado de Nivel Alto con DCCF portable o centralizado
- Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" habilitado.

En cualquier otro caso, se indicará en el propio certificado mediante los siguientes campos:

- Extensión "Certificate Policies" con valor OID de la política de certificación propia de Firmaprofesional correspondiente al certificado de Nivel Medio
- Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" deshabilitado.

1.4.2 Usos prohibidos de los certificados

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 esta CP y en la CPS.

Además, no se permite la utilización de los certificados de empleado público y empleado público con seudónimo para usos distintos de lo establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público para este tipo de certificados.

No se recomienda el uso de los certificados emitidos bajo esta Política para el cifrado de documentos.

1.5 Administración de Políticas

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

1.5.1 Organización que administra el documento

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

1.5.2 Persona de contacto

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

1.5.3 Persona que determina la idoneidad de la CP para la póliza

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

1.5.4 Procedimiento de aprobación de la CP

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

1.6 Definiciones y siglas

Según lo dispuesto en la Declaración de Prácticas de Certificación de Firmaprofesional (<http://www.firmaprofesional.com/cps>).

2. Repositorios y Publicación de la Información

2.1 Repositorios

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

2.2 Publicación de información de certificación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

2.3 Hora o frecuencia de publicación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

2.4 Control de acceso a los repositorios

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3. Identificación y Autenticación

3.1 Registro de Nombres

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

Los límites de los campos givenName, surname, pseudonym, commonName, and organizationName puede ser mayor que el límite establecido en RFC 5280, conforme a la ETSI 319 412-2 y ETSI 319 412-3.

3.1.1 Tipos de nombres

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3.1.2 Necesidad de que los nombres sean significativos

Los campos del DN referentes al Nombre y Apellidos se corresponderá con los datos registrados legalmente del firmante, expresados exactamente en el formato que conste en el Documento Nacional de Identidad, tarjeta de residencia, pasaporte u otro medio admitido en derecho.

3.1.3 Anonimato o seudónimo de los suscriptores

Únicamente los certificados del tipo "certificados de empleado público con seudónimo o con número de identificación profesional" admiten el uso de seudónimo.

3.1.4 Reglas para interpretar varias formas de nombres

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3.1.5 Unicidad de los nombres

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3.1.6 Reconocimiento, autenticación y función de las marcas

Sin estipulación

3.2 Validación inicial de la identidad

3.2.1 Método de prueba de posesión de clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional

3.2.2 Autenticación de la identidad de la organización e identidad de dominio

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3.2.3 Autenticación de la identidad de una persona física

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3.2.4 Información de suscriptor no verificada

Sin estipulación.

3.2.5 Validación de la identidad de la RA y de operadores de la RA

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

3.2.6 Criterios de interoperabilidad

En la actualidad Firmaprofesional no dispone de certificación cruzada.

3.3 Identificación y autenticación para solicitudes de renovación de claves

3.3.1 Identificación y autenticación para el cambio de clave

Se deben seguir los mismos pasos que para la emisión de un nuevo certificado (4.3 Emisión de certificados).

3.3.2 Identificación y autenticación para la renovación de certificados tras su revocación

Se deben seguir los mismos pasos que para la emisión de un nuevo certificado (4.3 Emisión de certificados).

3.4 Identificación y autenticación para solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4. Requisitos operativos del ciclo de vida del certificado

4.1. Solicitud del certificado

4.1.1 Quién puede enviar una solicitud de certificado

Las solicitudes de estos certificados se realizan por personas físicas a través de las Autoridades de Registro de Firmaprofesional.

4.1.2 Proceso de solicitud de certificados y responsabilidades

Los pasos a seguir para la obtención del certificado son los siguientes:

Por regla general, las solicitudes de los certificados contenidos en la presente CP, podrán realizarse a Firmaprofesional dirigiéndose a algún colaborador que actúe como RA de Firmaprofesional.

En el caso de Certificados Corporativos de Persona Física, Certificados Corporativos de Colegiado, Certificados de Empleado Público y Certificados de empleado público con seudónimo o número de identificación profesional, la Corporación o la Administración Pública que actúe como RA de Firmaprofesional podrá tramitar directamente las solicitudes y proceder a la emisión de los certificados accediendo a los sistemas de gestión y emisión de certificados de Firmaprofesional. Para ello, el usuario que desee solicitar un certificado deberá ponerse en contacto con su Organización y realizar la solicitud como así se establezca.

En el caso de Certificados Personales, la solicitud también se podrá realizar mediante el uso de un certificado electrónico cualificado vigente, siempre que Firmaprofesional pueda comprobar de forma automatizada la fecha de la última personación del Solicitante ante el Prestador de Servicios de Confianza con cuyo certificado se realiza la solicitud.

4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

Es responsabilidad de la RA realizar la identificación y autenticación del firmante. Este proceso deberá ser realizado previamente a la emisión del certificado.

4.2.2 Aprobación o denegación de las solicitudes de certificados

La RA de Firmaprofesional (en su caso, el Organismo Público, el Colegio Profesional o la Corporación correspondiente), deberá comprobar la veracidad de los datos suministrados por el solicitante.

Dependiendo del tipo de certificado, esta verificación se realizará mediante uno de los siguientes métodos:

- a. Certificados corporativos de colegiado: el solicitante deberá estar colegiado en el Colegio Profesional.
- b. Certificados corporativos de persona física: La Corporación que actúe como RA podrá establecer los requisitos necesarios que deben cumplir sus usuarios. La Corporación que actúe como RA únicamente podrá tramitar solicitudes de firmantes vinculados a su propia Corporación.

Las solicitudes de estos certificados que se realicen directamente a Firmaprofesional deberán adjuntar un documento firmado, manual o digitalmente, por el Responsable Legal de Corporación por el que se autorice la emisión de estos certificados y se indique el Nombre, Apellidos, DNI y Cargo en la organización de cada persona autorizada. El solicitante podrá solicitar certificados exclusivamente a aquellas personas que tenga identificadas previamente a través de sus procedimientos internos, y que no hayan pasado más de 5 años desde la última identificación, de esta forma no es necesario que el firmante se deba personar ante Firmaprofesional.

En caso de tratarse de un empresario individual únicamente se requerirá que el solicitante aporte la documentación necesaria que demuestre que está dado de alta en Seguridad Social como tal, como un recibo bancario con el pago correspondiente.

- c. Certificados corporativos de Representante sin personalidad jurídica. Se verificará mediante uno de los siguientes métodos:
 - Consulta telemática al Registro Mercantil.
 - Revisión de la documentación notarial aportada.
 - Revisión del boletín oficial indicado por el solicitante
 - En caso de no aplicar ninguno de los puntos anteriores, revisión de la documentación aportada acreditativa de representación de entidad sin personalidad jurídica.
- d. Certificados corporativos de Representante legal y de representante voluntario. Se verificará mediante una consulta telemática al Registro Mercantil o bien revisando la documentación notarial aportada o el boletín oficial indicado por el solicitante.
- e. Certificados Personales. La verificación podrá no ser exigible en los siguientes casos

- cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados le constaran a la RA en virtud de una relación preexistente, en la que para la identificación del interesado, se hubieran empleado los medios señalados en esta sección y el período de tiempo transcurrido desde la identificación sea menor de cinco años.
 - Cuando para solicitar un certificado se utilice otro certificado vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en apartado anterior y le conste a la RA que el período de tiempo transcurrido desde la identificación es menor de cinco años.
- f. Certificados de empleado público: la Organización validará la identidad del solicitante y su condición de empleado público.

4.2.3 Tiempo de tramitación de las solicitudes de certificado

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.3 Emisión de certificados

Cada Autoridad de Registro de Firmaprofesional tendrá acreditadas a una serie de personas para actuar como Operador de RA frente a FirmaProfesional (independientemente de que la RA sea un Colegio Profesional o un Organismo Público). Estos Operadores de RA habrán sido autorizados por la RA para realizar esta función siendo previamente instruidos en la operativa de emisión de certificados. Cada Operador de RA dispondrá de un Certificado Digital en Dispositivo Criptográfico Seguro, que le permitirá gestionar las solicitudes de certificados de usuarios.

4.3.1 Acciones de la CA durante la emisión del certificado

En los Certificados Personales, una vez sea aceptada la solicitud, y previo a la emisión del certificado, Firmaprofesional tomará las medidas razonables para comprobar la validez del correo electrónico proporcionado por el solicitante, como por ejemplo a través del intercambio de correo con la solicitud de documentación requerida para la emisión de dicho certificado o enviando un dato aleatorio al que el solicitante debe acceder para demostrar la existencia del correo-e.

Una vez se haya comprobado el correo, se le enviará al solicitante la información necesaria para que pueda generar el par de claves en sus sistemas, previa autenticación del mismo. Firmaprofesional recibirá la solicitud de certificado automáticamente tras la generación de las claves, emitirá el certificado y proveerá los medios para que el solicitante lo instale en sus sistemas.

Sin embargo, para el resto de Certificados contenidos en esta Política, es preciso diferenciar tres fases:

a) Generación de claves

En caso necesario, el Operador de RA gestionará la generación de claves para el firmante en un dispositivo de creación firma.

El Operador de RA validará que el firmante está en posesión de la clave privada (datos de creación de firma) asociada a la clave pública (datos de verificación de firma) incluida en la petición de certificación.

b) Emisión del certificado

El Operador de RA generará la petición de certificado en un formato estándar y la enviará a Firmaprofesional.

Firmaprofesional validará la integridad de la petición y que ha sido generada por un Operador de RA debidamente autorizado. Tras esta validación se procederá a la emisión del certificado.

En los casos en que Firmaprofesional tenga garantía de que el dispositivo en el que se han generado el par de claves es un DCCF, el certificado se emitirá con el OID correspondiente.

c) Entrega

Una vez se ha generado el certificado, y antes de que la RA pueda entregarlo al firmante, éste último deberá:

- Personarse ante la RA en cumplimiento del artículo 7 de la Ley 6/2020 LSEC, salvo en los casos en que esta personación no sea necesaria tal como recoge el propio artículo.

- Aceptar formalmente la entrega del certificado dejando evidencia documental en poder de la RA.

Finalmente, la RA hará entrega del certificado al firmante, ya sea entregando el DCCF portable, los mecanismos de autenticación y operación remota, o habilitando los mecanismos para su descarga y posterior uso.

En los Certificados Corporativos de Persona Física y, en el caso de que el solicitante actúe en representación de otra persona física, se deberá obtener la aceptación del certificado por parte del firmante antes de que el certificado pueda ser considerado válido. En este caso, el certificado se emitirá con un período de carencia durante el cual el certificado no será válido. Finalizado el período de carencia, si el solicitante dispone de los medios para acceder a la clave privada y no ha conseguido la aceptación formal del certificado por parte del firmante, el solicitante deberá revocar el certificado de inmediato. En caso contrario, se le considerará responsable de todos los perjuicios que puedan ocasionarse por el uso del certificado, especialmente los referentes a la protección de datos de carácter personal del firmante.

Mediante estos procedimientos Firmaprofesional garantiza que ningún firmante dispone del certificado antes de que se haya realizado el proceso de personación requerido en el artículo 7 de la Ley 6/2020 LSEC.

4.3.2 Notificación al suscriptor por parte de la CA de la emisión del certificado y entrega

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.4 Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.4.2 Publicación del certificado por la CA

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.4.3 Notificación de la emisión del certificado por parte de la CA a otras entidades

Sin estipulación.

4.5 Uso de la claves y del certificado

4.5.1 Uso de certificado y clave privada del suscriptor

Los certificados emitidos bajo la presente CP pueden ser utilizados para identificar al suscriptor y para firmar documentos y ficheros electrónicos.

4.5.2 Uso de certificados y claves públicas de parte que confía

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente CP y la CPS.

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por Firmaprofesional concretamente para ello y especificados en la CPS.

4.6 Renovación del certificado (sin cambio de claves)

Sin estipulación salvo cuando exista cambio de claves que se regirá por lo establecido en el punto 4.7.

4.6.1 Circunstancia para la renovación del certificado

Sin estipulación.

4.6.2 Quién puede solicitar la renovación

Sin estipulación.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Sin estipulación.

4.6.4 Notificación al suscriptor de la emisión de un nuevo certificado

Sin estipulación.

4.6.5 Conducta que constituye la aceptación de un certificado de renovación

Sin estipulación.

4.6.6 Publicación del certificado de renovación por parte de la CA

Sin estipulación.

4.6.7 Notificación de la emisión del certificado por parte de la CA a otras entidades

Sin estipulación.

4.7 Renovación del certificado con cambio de clave

4.7.1 Circunstancia para el cambio de clave del certificado

Solamente se podrá proceder a la renovación del certificado si se cumplen las condiciones siguientes:

- El certificado no ha caducado.
- En el caso de certificados cualificados, hayan transcurrido menos de 5 años desde su última personación e identificación ante la RA.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

Cualquier firmante podrá pedir la renovación de su certificado si se cumplen las circunstancias descritas en el punto anterior.

4.7.3 Procesamiento de solicitudes de cambio de claves de certificados

La renovación del certificado se puede realizar a través de los siguientes procedimientos:

1. Presencial: el firmante deberá dirigirse personalmente a la RA de Firmaprofesional y solicitar un certificado nuevo.
2. Online: si la RA dispone del servicio, el firmante deberá conectarse al servicio online que ofrece Firmaprofesional con su certificado actual aún vigente y firmar electrónicamente la solicitud de renovación o disponer de algún otro mecanismo que permita autenticar su identidad y voluntad de renovar el certificado. La posibilidad de realizar la renovación online estará condicionada por los requisitos que establezca la legislación vigente en materia de firma electrónica. El período de validez de los certificados renovados online estará condicionado por los requisitos que establece el artículo 7 de la Ley 6/2020 LSEC.
3. Automático (únicamente para Certificados Personales): si el firmante acepta esta posibilidad en el momento de emisión del certificado, antes de que caduque el certificado vigente se generará automáticamente un nuevo certificado con las mismas claves. La posibilidad de realizar la renovación automática estará condicionada por lo que establezca la legislación vigente en materia de firma electrónica.

4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.7.5 Conducta que constituye la aceptación de un certificado con clave nueva

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.7.6 Publicación del certificado con nueva clave por parte de la CA

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.8 Modificación del certificado

En caso de necesidad de modificar algún dato, la RA deberá proceder a la revocación y a la emisión de un nuevo certificado.

4.8.1 Circunstancia para la modificación del certificado

Sin estipulación.

4.8.2 Quién puede solicitar la modificación del certificado

Sin estipulación.

4.8.3 Procesamiento de solicitudes de modificación de certificados

Sin estipulación.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

Sin estipulación.

4.8.5 Conducta que constituye la aceptación del certificado modificado

Sin estipulación.

4.8.6 Publicación del certificado modificado por la CA

Sin estipulación.

4.8.7 Notificación de la emisión del certificado por parte de la CA a otras entidades

Sin estipulación.

4.9 Revocación y suspensión de certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.1 Circunstancias para la revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.2 Quién puede solicitar la revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.3 Procedimiento de solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.4 Periodo de gracia de la solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.6 Requisito de verificación de revocación para las partes que confían

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.7 Frecuencia de emisión de CRL

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.8 Latencia máxima para las CRL

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.9 Disponibilidad de verificación de estado / revocación en línea

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.10 Requisitos de verificación de revocación en línea

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.11 Otras formas de anuncios de revocación disponibles

Sin estipulación.

4.9.12 Requisitos especiales relacionados con el compromiso clave

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.13 Circunstancias para la suspensión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.14 Quién puede solicitar la suspensión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.15 Procedimiento de solicitud de suspensión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.9.16 Límites del período de suspensión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.10 Servicios de estado de certificados

4.10.1 Características operativas

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.10.2 Disponibilidad del servicio

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.10.3 Funciones opcionales

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.11 Finalización de la suscripción

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.12 Custodia y recuperación de claves

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

4.12.1 Política y prácticas de custodia y recuperación de claves

Sin estipulación.

4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión

Sin estipulación.

5. Controles de seguridad física, instalaciones, gestión y operacionales

5.1 Controles físicos

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.1 Ubicación y construcción del sitio

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.2 Acceso físico

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.3 Energía y aire acondicionado

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.4 Exposición al agua

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.5 Prevención y protección contra incendios

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.6 Almacenamiento de medios

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.7 Eliminación de residuos

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.1.8 Respaldo fuera de las instalaciones

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.2 Controles de procedimiento

5.2.1 Roles de confianza

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.2.2 Número de personas necesarias por tarea

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.2.3 Identificación y autenticación para cada rol

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.2.4 Roles que requieren separación de funciones

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3 Controles de personal

5.3.1 Calificaciones, experiencia y requisitos de autorización

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3.2 Procedimientos de verificación de antecedentes

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3.3 Requisitos de formación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3.4 Frecuencia y requisitos de reentrenamiento

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3.5 Frecuencia y secuencia de la rotación del trabajo

Sin estipulación.

5.3.6 Sanciones por acciones no autorizadas

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3.7 Requisitos de los contratistas independientes

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.3.8 Documentación suministrada al personal

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4 Procedimientos de registro de auditorías

5.4.1 Tipos de eventos registrados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4.2 Frecuencia de procesado de registros de auditoría

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4.3 Período de conservación del registros de auditoría

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4.4 Protección de los registros de auditoría

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4.6 Sistema de recogida de auditorías

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.4.7 Notificación al sujeto causante del evento

Sin estipulación.

5.4.8 Análisis de vulnerabilidades

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.5 Archivo de registros

5.5.1 Tipos de registros archivados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.5.2 Período de conservación del archivo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.5.3 Protección del archivo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.5.4 Procedimientos de copia de seguridad del archivo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.5.5 Requisitos para el sellado de tiempo de los registros

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.5.6 Sistema de recogida de archivos

Sin estipulación.

5.5.7 Procedimientos para obtener y verificar la información del archivo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.6 Cambio de claves

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.7 Plan de recuperación de desastres

5.7.1 Procedimientos de gestión de incidentes y compromisos

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.7.2 Los recursos informáticos, el software y/o los datos se corrompen

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.7.3 Procedimientos de compromiso de la clave privada de la entidad

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.7.4 Capacidades de continuidad del negocio después de un desastre

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

5.8 Cese de la actividad de la RA o CA

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

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 Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.1.2 Entrega de la clave privada al suscriptor

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.1.3 Entrega de la clave pública al emisor del certificado

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.1.4 Entrega de la clave pública de la CA a las partes confiantes

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.1.5 Tamaño de las claves

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.1.6 Generación de parámetros de clave pública y control de calidad

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.1.7 Propósitos de uso de la clave (según el campo de uso de la clave X.509 v3)

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2 Protección de la clave privada y controles de ingeniería del módulo criptográfico

6.2.1 Normas y controles del módulo criptográfico

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.2 Control multipersona (k de n) de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.3 Depósito de claves privadas

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.4 Copia de seguridad de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.5 Archivo de claves privadas

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.6 Transferencia de claves privadas hacia o desde un módulo criptográfico

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.8 Método de activación de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.9 Método de desactivación de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.10 Método de destrucción de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.2.11 Clasificación del módulo criptográfico

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.3 Otros aspectos de la gestión de pares de claves

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.3.1 Archivo de la clave pública

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.3.2 Periodos de funcionamiento del certificado y períodos de uso del par de claves

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.4 Datos de activación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.4.1 Generación e instalación de datos de activación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.4.2 Protección de los datos de activación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.4.3 Otros aspectos de los datos de activación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.5 Controles de seguridad informática

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.5.1 Requisitos técnicos específicos de seguridad informática

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.5.2 Evaluación de la seguridad informática

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo del sistema

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.6.2 Controles de gestión de la seguridad

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.6.3 Controles de seguridad del ciclo de vida

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.7 Controles de seguridad de la red

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

6.8 Control de tiempo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7. Perfiles de los certificados , CRL y OCSP

7.1 Perfil del certificado

7.1.1 Número(s) de versión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.1.2 Extensiones del certificado

Las extensiones utilizadas por cada tipo de certificado emitidos bajo la presente política se publican en el documento denominado "Perfiles de los certificados de Firmaprofesional" en la web de Firmaprofesional (<http://www.firmaprofesional.com/cps>).

7.1.3 Identificadores de objetos de algoritmos

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.1.4 Formas del nombre

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.1.5 Restricciones del nombre

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.1.6 Identificador del objeto de la política del certificado

Al amparo de las prescripciones contenidas en la presente Política de Certificación se emiten los siguientes tipos de certificados, con sus OID asociados:

Tipo de Certificado	OID
Certificados Corporativos de Colegiado. Nivel alto con DCCF portable	1.3.6.1.4.1.13177.10.1.1.1
Certificados Corporativos de Colegiado. Nivel alto con DCCF centralizado	1.3.6.1.4.1.13177.10.1.1.3
Certificados Corporativos de Colegiado. En otros dispositivos	1.3.6.1.4.1.13177.10.1.1.2
Certificados Corporativos de Persona Física. Nivel alto con DCCF portable	1.3.6.1.4.1.13177.10.1.2.1
Certificados Corporativos de Persona Física. Nivel alto con DCCF centralizado	1.3.6.1.4.1.13177.10.1.2.3

Certificados Corporativos de Persona Física. En otros dispositivos	1.3.6.1.4.1.13177.10.1.2.2
Certificados Corporativos de Persona Física con firma de correo. En otros dispositivos	1.3.6.1.4.1.13177.10.1.14.2
Certificados Corporativos de Representante Legal.En DCCF portable	1.3.6.1.4.1.13177.10.1.11.1
Certificados Corporativos de Representante Legal. En DCCF centralizado	1.3.6.1.4.1.13177.10.1.11.3
Certificados Corporativos de Representante Legal. En otros dispositivos	1.3.6.1.4.1.13177.10.1.11.2
Certificados Corporativos de Representante Voluntario frente a las Administraciones Públicas. En DCCF portable	1.3.6.1.4.1.13177.10.1.12.1
Certificados Corporativos de Representante Voluntario frente a las Administraciones Públicas. En DCCF centralizado.	1.3.6.1.4.1.13177.10.1.12.3
Certificados Corporativos de Representante Voluntario frente a las Administraciones Públicas. En otros dispositivos.	1.3.6.1.4.1.13177.10.1.12.2
Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica. En DCCF portable	1.3.6.1.4.1.13177.10.1.13.1
Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica. En DCCF centralizado	1.3.6.1.4.1.13177.10.1.13.3

Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica. En otros dispositivos	1.3.6.1.4.1.13177.10.1.13.2
Certificados de Empleado Público. Nivel Alto con DCCF portable	1.3.6.1.4.1.13177.10.1.22.1
Certificados de Empleado Público. Nivel Alto con DCCF centralizado	1.3.6.1.4.1.13177.10.1.22.3
Certificados de Empleado Público. Nivel Medio	1.3.6.1.4.1.13177.10.1.22.2
Certificados de empleado público con seudónimo o con número de identificación profesional	1.3.6.1.4.1.13177.10.1.23.2
Certificados Personales. En otros dispositivos	1.3.6.1.4.1.13177.10.1.40.2
Certificados Personales. En DCCF centralizado	1.3.6.1.4.1.13177.10.1.40.3

7.1.7 Uso de la extensión Policy Constraints

Sin estipulación.

7.1.8 Sintaxis y semántica de los calificadores de política

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.1.9 Semántica de procesamiento de la extensión critical Certificate Policies

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.2 Perfil CRL

7.2.1 Número(s) de versión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.2.2 Extensiones de CRL y entradas de CRL

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.3 Perfil OCSP

7.3.1 Número(s) de versión

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

7.3.2 Extensiones OCSP

Sin estipulación.

8. Auditorías de cumplimiento y otros controles

8.1 Frecuencia de las auditorías

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

8.2 Cualificación del auditor o evaluador

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

8.3 Relación entre el auditor y la autoridad auditada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

8.4 Aspectos cubiertos por la evaluación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

8.5 Acciones a emprender como resultado de la detección de deficiencias

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9. Otras cuestiones legales y de la actividad

9.1 Tarifas

Firmaprofesional cobrará al Suscriptor lo acordado en el contrato de prestación de servicios firmado por las partes.

Firmaprofesional podrá establecer las tarifas que considere oportunas a los suscriptores, así como establecer los medios de pago que considere más adecuado en cada caso. Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar con el Departamento Comercial de Firmaprofesional.

9.1.1 Tarifas de emisión o renovación de certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.1.2 Tarifas de acceso a los certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.1.3 Tarifas de acceso a la información de revocación o de estado

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.1.4 Tarifas por otros servicios

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.1.5 Tarifas de reembolso

Sin estipulación.

9.2 Responsabilidades económicas

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.2.1 Cobertura del seguro

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro o garantía para las entidades finales

Sin estipulación.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.3.2 Información no confidencial

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.3.3 Responsabilidad de proteger la información confidencial

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4 Protección de la información personal

9.4.1 Política de protección de datos de carácter personal

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4.2 Información tratada como privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4.3 Información no considerada privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4.4 Responsabilidad de proteger la información privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4.5 Aviso y consentimiento para el uso de la información privada

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4.6 Divulgación en virtud de un proceso judicial o administrativo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.4.7 Otras circunstancias de divulgación de información

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.5 Derechos de propiedad intelectual

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.6 Obligaciones y garantías

9.6.1 Obligaciones de la AC

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.6.2 Obligaciones de la AR

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.6.3 Obligaciones de los solicitantes

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.6.4 Representaciones y garantías de los terceros que confían en los certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.6.5 Declaraciones y garantías de otros participantes

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.7 Exención de garantía

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.8 Limitaciones de responsabilidad

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.9 Indemnizaciones

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.10 Periodo de validez y terminación

9.10.1 Plazo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.10.2 Terminación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.10.3 Efecto de la terminación y supervivencia

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.11 Avisos y comunicaciones individuales con los participantes

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.12 Modificaciones o cambios en las especificaciones

9.12.1 Procedimiento para los cambios

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.12.2 Mecanismo y plazo de notificación

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.12.3 Circunstancias en las que debe modificarse la OID

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.13 Disposiciones para la resolución de conflictos

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.14 Normativa aplicable

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.15 Cumplimiento de la normativa aplicable

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.16 Disposiciones diversas

9.16.1 Acuerdo completo

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.16.2 Independencia

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.16.3 Resolución por vía judicial

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)

Sin estipulación.

9.16.5 Fuerza mayor

Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.

9.17 Otras disposiciones

Sin estipulación.