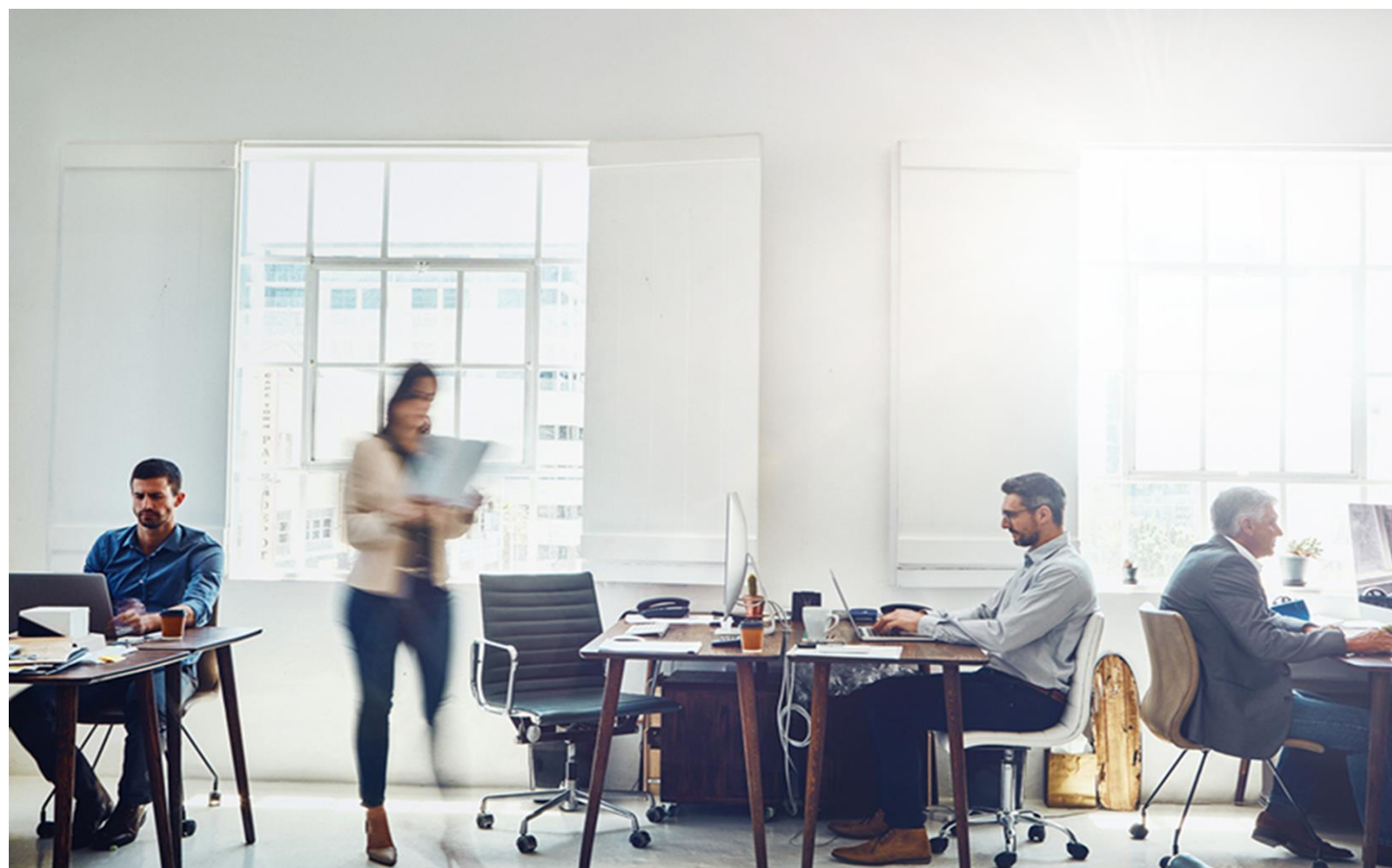


Política de Certificación

Certificados de Sello Electrónico

Versión: 230616

Clasificación: Público



Histórico de versiones

Versión	Sección y cambios	Fecha de publicación
190121	<ul style="list-style-type: none"> Nueva Política de Certificación de Certificados de Sello Electrónico 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"> Homogeneización de la terminología del Sello de AAPP a Sello de Órgano. Aumento del periodo de validez de los certificados de sello de órgano, pasando de 3 a 5 años. Comprobación del correo electrónico del solicitante previa a la emisión del certificado Cambio de la CA que emite los certificados de Sello de Órgano a "AC Firmaprofesional - CUALIFICADOS". 	07/05/2019
190612	<ul style="list-style-type: none"> Inclusión de certificados de sello para servicios de pago basados en la Directiva de servicios de pago 2015/2366 (PSD2) 	12/06/2019
200417	<ul style="list-style-type: none"> Incorporación de medidas por Estado de Alarma del COVID-19 	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 RFC 3647 Revisión general 	16/02/2022
230216	<ul style="list-style-type: none"> Revisión general 	16/02/2023
230616	<ul style="list-style-type: none"> ∅ Nuevo perfil de Sello Empresarial en DCCF Centralizado 	16/06/2023

Índice

1. Introducción	12
1.1. Resumen	12
1.2. Identificación del Documento	13
1.3. Entidades participantes	14
1.3.1 Autoridades de Certificación (CA)	14
1.3.2. Autoridad de Registro (RA)	14
1.3.3 Suscriptores	15
1.3.3.1 Solicitante	15
1.3.4. Tercero que confía en los certificados	15
1.3.5. Otros participantes	16
1.4 Uso de los certificados	16
1.4.1 Usos apropiados de los certificados	16
1.4.1.1. Periodo de validez de los certificados.....	17
1.5 Administración de Políticas	17
1.5.1 Organización que administra el documento	17
1.6 Definiciones y siglas	18
2. Repositorios y Publicación de la Información	18
2.1 Repositorios.....	18
3. Identificación y Autenticación	19
3.1 Registro de Nombres	19
3.1.1 Tipos de nombres.....	19
3.2.1 Método de prueba de posesión de clave privada.....	20
3.3.1 Identificación y autenticación para el cambio de clave	21
4. Requisitos operativos del ciclo de vida del certificado	21
4.1. Solicitud del certificado	21
4.1.1 Quién puede enviar una solicitud de certificado.....	21
4.2 Tramitación de las solicitudes de certificados.....	23

4.2.1 Realización de las funciones de identificación y autenticación	23
4.2.2 Aprobación o denegación de las solicitudes de certificados.....	23
4.2.3. Tiempo de tramitación de las solicitudes de certificado.....	23
4.3 Emisión de certificados	23
4.3.1 Acciones de la CA durante la emisión del certificado	23
4.3.2 Notificación al suscriptor por parte de la CA de la emisión del certificado	25
4.4.1 Forma en la que se acepta el certificado	25
4.4.2 Publicación del certificado por la CA	25
4.4.3 Notificación de la emisión del certificado por parte de la CA a otras entidades....	25
4.5 Uso de la claves y del certificado	25
4.5.1 Uso de certificado y clave privada del suscriptor.....	25
4.5.2 Uso de certificados y claves públicas por las partes que confían en los certificados	26
4.6. Renovación de certificados sin cambio de claves	26
4.6.1. Circunstancia para la renovación del certificado	26
4.6.2. Quién puede solicitar la renovación	26
4.6.3. Proceso de solicitudes de renovación de certificados.....	26
4.6.4. Notificación al suscriptor de la emisión de un nuevo certificado	26
4.6.5. Conducta que constituye la aceptación de un certificado de renovación	26
4.6.6. Publicación del certificado de renovación por parte de la CA	26
4.6.7. Notificación de la emisión del certificado por parte de la CA a otras entidades...	27
4.7 Renovación del certificado con cambio de claves	27
4.7.1 Circunstancia para el cambio de clave del certificado.....	27
4.7.2 Quién puede solicitar la certificación de una nueva clave pública	27
4.7.3 Procesamiento de solicitudes de cambio de claves de certificados.....	27
4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado	27
4.7.5 Conducta que constituye la aceptación de un certificado con clave nueva	28
4.7.6 Publicación del certificado con nueva clave por parte de la CA	28
4.8 Modificación del certificado	28
4.8.1. Circunstancia de la modificación del certificado.....	28

4.8.2. Quién puede solicitar la modificación del certificado	28
4.8.3. Tramitación de solicitudes de modificación de certificados	28
4.8.4. Notificación de la emisión de un nuevo certificado al suscriptor	28
4.8.5. Comportamiento que constituye la aceptación de un certificado modificado	28
4.8.6. Publicación del certificado modificado por la AC	29
4.8.7. Notificación de la expedición de certificados por la AC a otras entidades	29
4.9 Revocación y suspensión de certificados.....	29
4.9 Revocación y suspensión de certificados.....	29
4.9.1 Circunstancias para la revocación.....	29
4.9.2 Quién puede solicitar la revocación	29
4.9.3 Procedimiento de solicitud de revocación	29
4.9.4 Periodo de gracia de la solicitud de revocación.....	30
4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación.....	30
4.9.6 Requisito de verificación de revocación para las partes que confían	30
4.9.7 Frecuencia de emisión de CRL.....	30
4.9.8 Latencia máxima para las CRL.....	30
4.9.9 Disponibilidad de verificación de estado / revocación en línea	30
4.9.10 Requisitos de verificación de revocación en línea.....	30
4.9.11 Otras formas de anuncios de revocación disponibles.....	31
4.9.12 Requisitos especiales relacionados con el compromiso clave.....	31
4.9.16 Límites del período de suspensión.....	31
4.10 Servicios de estado de certificados.....	31
4.10.1 Características operativas	31
4.10.2 Disponibilidad del servicio	32
4.10.3 Funciones opcionales	32
4.11 Finalización de la suscripción.....	32
4.12 Custodia y recuperación de claves	32
4.12.1 Política y prácticas de custodia y recuperación de claves.....	32
4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión	32

5. Controles de seguridad física, instalaciones, gestión y operacionales	33
5.1 Controles físicos.....	33
5.1.1 Ubicación y construcción del sitio	33
5.1.2 Acceso físico	33
5.1.3 Energía y aire acondicionado	33
5.1.4 Exposición al agua	33
5.1.5 Prevención y protección contra incendios	33
5.1.6 Almacenamiento de medios.....	34
5.1.7 Eliminación de residuos.....	34
5.1.8 Respaldo fuera de las instalaciones	34
5.2 Controles de procedimiento.....	34
5.2.1 Roles de confianza	34
5.2.2 Número de personas necesarias por tarea	34
5.2.3 Identificación y autenticación para cada rol.....	34
5.2.4 Roles que requieren separación de funciones.....	35
5.3 Controles de personal.....	35
5.3.1 Calificaciones, experiencia y requisitos de autorización.....	35
5.3.2 Procedimientos de verificación de antecedentes.....	35
5.3.3 Requisitos de formación	35
5.3.4 Frecuencia y requisitos de reentrenamiento	35
5.3.5 Frecuencia y secuencia de la rotación del trabajo.....	35
5.3.6 Sanciones por acciones no autorizadas	35
5.3.7 Requisitos de los contratistas independientes	36
5.3.8 Documentación suministrada al personal	36
5.4 Procedimientos de registro de auditorías.....	36
5.4.1 Tipos de eventos registrados	36
5.4.2 Frecuencia de procesado de registros de auditoría.....	36
5.4.3 Período de conservación del registros de auditoría.....	36
5.4.4 Protección de los registros de auditoría	36

5.4.5 Procedimientos de respaldo de los registros de auditoría	37
5.4.6 Sistema de recogida de auditorías	37
5.4.7 Notificación al sujeto causante del evento	37
5.4.8 Análisis de vulnerabilidades	37
5.5 Archivo de registros	37
5.5.1 Tipos de registros archivados	37
5.5.2 Período de conservación del archivo	37
5.5.3 Protección del archivo	37
5.5.4 Procedimientos de copia de seguridad del archivo	38
5.5.5 Requisitos para el sellado de tiempo de los registros	38
5.5.6 Sistema de recogida de archivos	38
5.5.7 Procedimientos para obtener y verificar la información del archivo	38
5.6 Cambio de claves	38
5.7 Plan de recuperación de desastres	38
5.7.1 Procedimientos de gestión de incidentes y compromisos	38
5.8 Cese de la actividad de la RA o CA	39
6. Controles de seguridad técnica	39
6.1 Generación e instalación del par de claves	39
6.1.1 Generación del par de claves	39
6.1.2 Entrega de la clave privada al suscriptor	39
6.1.3 Entrega de la clave pública al emisor del certificado	39
6.1.5 Tamaño de las claves	40
6.2 Protección de la clave privada y controles de ingeniería del módulo criptográfico	40
6.2.2 Control multipersona (k de n) de la clave privada	40
6.2.3 Depósito de claves privadas	41
6.2.4 Copia de seguridad de la clave privada	41
6.2.5 Archivo de claves privadas	41
6.2.6 Transferencia de claves privadas hacia o desde un módulo criptográfico	41
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico	41

6.2.8 Método de activación de la clave privada	41
6.2.9 Método de desactivación de la clave privada	41
6.2.10 Método de destrucción de la clave privada	42
6.2.11 Clasificación del módulo criptográfico	42
6.3 Otros aspectos de la gestión de pares de claves	42
6.3.1 Archivo de la clave pública	42
6.3.2 Periodos de funcionamiento del certificado y períodos de uso del par de claves..	42
6.4 Datos de activación.....	42
6.4.1 Generación e instalación de datos de activación	42
6.4.2 Protección de los datos de activación	43
6.4.3 Otros aspectos de los datos de activación	43
6.5 Controles de seguridad informática	43
6.5.1 Requisitos técnicos específicos de seguridad informática	43
6.5.2 Evaluación de la seguridad informática	43
6.6 Controles técnicos del ciclo de vida	43
6.6.1 Controles de desarrollo del sistema	43
6.6.2 Controles de gestión de la seguridad	44
6.6.3 Controles de seguridad del ciclo de vida	44
6.7 Controles de seguridad de la red	44
6.8 Control de tiempo	44
7. Perfiles de los certificados , CRL y OCSP.....	44
7.1 Perfil del certificado	44
7.1.1 Número(s) de versión	44
7.1.2 Extensiones del certificado.....	45
7.1.3 Identificadores de objetos de algoritmos	45
7.1.4 Formas del nombre	45
7.1.5 Restricciones del nombre	45
7.1.6 Identificador del objeto de la política del certificado	45
7.1.7 Uso de la extensión Policy Constraints	46

7.1.8 Sintaxis y semántica de los calificadores de política	46
7.1.9 Semántica de procesamiento de la extensión critical Certificate Policies.....	46
7.2 Perfil CRL.....	46
7.2.1 Número(s) de versión	46
7.2.2 Extensiones de CRL y entradas de CRL	46
7.3 Perfil OCSP	47
7.3.1 Número(s) de versión	47
7.3.2 Extensiones OCSP	47
8. Auditorías de cumplimiento y otros controles	48
8.1 Frecuencia de las auditorías	48
8.2 Cualificación del auditor o evaluador	48
8.3 Relación entre el auditor y la autoridad auditada.....	48
8.4 Aspectos cubiertos por la evaluación.....	48
8.5 Acciones a emprender como resultado de la detección de deficiencias	48
9. Otras cuestiones legales y de la actividad	49
9.1 Tarifas.....	49
9.1.1 Tarifas de emisión o renovación de certificados	49
9.1.2 Tarifas de acceso a los certificados.....	49
9.1.3 Tarifas de acceso a la información de revocación o de estado	49
9.1.4 Tarifas por otros servicios.....	49
9.1.5 Tarifas de reembolso	49
9.2 Responsabilidades económicas.....	50
9.2.1 Cobertura del seguro.....	50
9.2.2 Otros activos.....	50
9.2.3 Cobertura de seguro o garantía para las entidades finales	50
9.3 Confidencialidad de la información comercial	50
9.3.1 Alcance de la información confidencial	50
9.3.2 Información no confidencial.....	50
9.3.3 Responsabilidad de proteger la información confidencial.....	50

9.4 Protección de la información personal	51
9.4.1 Política de protección de datos de carácter personal	51
9.4.2 Información tratada como privada.....	51
9.4.3 Información no considerada privada	51
9.4.4 Responsabilidad de proteger la información privada	51
9.4.5 Aviso y consentimiento para el uso de la información privada.....	51
9.4.6 Divulgación en virtud de un proceso judicial o administrativo	51
9.4.7 Otras circunstancias de divulgación de información	52
9.5 Derechos de propiedad intelectual	52
9.6 Obligaciones y garantías.....	52
9.6.1 Obligaciones de la AC	52
9.6.2 Obligaciones de la AR	52
9.6.3 Obligaciones de los solicitantes	52
9.6.4 Representaciones y garantías de los terceros que confían en los certificados	52
9.6.5 Declaraciones y garantías de otros participantes.....	53
9.7 Exención de garantía.....	53
9.8 Limitaciones de responsabilidad	53
9.9 Indemnizaciones	53
9.10 Periodo de validez y terminación.....	53
9.10.1 Plazo	53
Según lo dispuesto en la Declaración de Prácticas de Certificación vigente de Firmaprofesional.....	
9.10.2 Terminación	53
9.10.3 Efecto de la terminación y supervivencia	54
9.11 Avisos y comunicaciones individuales con los participantes	54
9.12 Modificaciones o cambios en las especificaciones.....	54
9.12.1 Procedimiento para los cambios	54
9.12.2 Mecanismo y plazo de notificación	54
9.12.3 Circunstancias en las que debe modificarse la OID	54
9.13 Disposiciones para la resolución de conflictos	54

9.14 Normativa aplicable	55
9.15 Cumplimiento de la normativa aplicable	55
9.16 Disposiciones diversas	55
9.16.1 Acuerdo completo	55
9.16.2 Independencia	55
9.16.3 Resolución por vía judicial	55
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos).....	55
9.16.5 Fuerza mayor	56
9.17 Otras disposiciones	56

1. Introducción

1.1. Resumen

Firmaprofesional emite esta Política de Certificación de Certificados de Sello Electrónico, aunando diferentes políticas cuyos certificados tienen por finalidad firmar en nombre de la organización u órgano, documentos electrónicos de forma automática bajo la responsabilidad del suscriptor del certificado.

El presente documento representa las Políticas de Certificación para los certificados siguientes:

1. Certificados de Sello de Órgano (de Administración, órgano o entidad de derecho público)
2. Certificados Corporativos de Sello Empresarial
3. Certificados de Sello Electrónico para servicios de pago (certificados de sello electrónico para PSD2)

Los Certificados de Sello Electrónico son acordes al Anexo III del Reglamento UE 910/2014 que especifica los requisitos para los certificados cualificados de sello electrónico, que los define como "una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma su identidad". El objetivo de un sello electrónico es garantizar el origen y la integridad de unos datos. Su existencia tiene sentido para identificar a una entidad (pública o privada) u órgano de la Administración Pública y para firmar de forma automatizada.

Por la regulación normativa española, se puede hacer distinción entre:

- **Certificados de Sello de Administración, órgano o entidad de derecho público:** son certificados cualificados expedidos a Administraciones Públicas, órganos o entidades de derecho público para dispositivos informáticos, programas o aplicaciones, bajo la responsabilidad del suscriptor o titular del certificado, de acuerdo con las indicaciones del artículo 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **Certificados Corporativos de Sello Empresarial:** son certificados digitales cualificados, en los términos de la Ley 6/2020 LSEC, que identifican al suscriptor y firmante como una

Corporación con personalidad jurídica. Estos certificados se ajustan a los requisitos que impone la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público y han sido autorizados, entre otros usos, para su utilización en facturación electrónica y digitalización certificada por la Agencia Tributaria.

- **Certificados de Sello Electrónico para PSD2:** son certificados electrónicos cualificados que se utilizan para identificar al proveedor del servicio de pago y proporcionan evidencia de autenticidad e integridad de los datos sellados.

En el presente documento se exponen las condiciones particulares referentes a estos tipos de certificados. Esta 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:	Política de Certificación para Certificados de Sello Electrónico
Versión:	230616
Descripción:	Desarrollo de una Política de Certificación de Certificados de Sello Electrónico, donde se incluye tanto certificados de sello empresarial como certificados de sello de Administración, órgano o Entidad de Derecho Público y certificados de sello para PSD2
Fecha de Emisión:	16/06/2023
OIDs	1.3.6.1.4.1.13177.10.1.21.D (*) Sello de Administración, Órgano o Entidad de derecho público 1.3.6.1.4.1.13177.10.1.10.D (*) Sello Empresarial y certificados de Sello Electrónico para PSD2
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 siguiente Políticas, que quedan derogadas con la publicación de la versión 190121 de ésta:

- Política de Certificación de Certificados de Sello de Administración, Órgano o Entidad de Derecho Público. Versión 171121. Esta Política puede ser consultada en <https://www.firmaprofesional.com/cps>, en el apartado “Políticas y Prácticas de Certificación anteriores”.
- Política de Certificación de Certificados Corporativos de Sello Empresarial. Versión 171121. Esta Política puede ser consultada 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)

Estos certificados deben ser emitidos por Firmaprofesional como Prestador de Servicios de Confianza que emite certificados cualificados según la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante Ley 6/2020 LSEC y el Reglamento UE 910/2014 (eIDAS).

En concreto, las CA que emiten estos certificados, dependiendo del tipo, son:

- Los certificados de Sello Empresarial y los certificados de Sello de Administración, órgano o Entidad de Derecho son emitidos por “AC Firmaprofesional - CUALIFICADOS” o “FIRMAPROFESIONAL ICA B01 QUALIFIED 2022”

1.3.2. Autoridad de Registro (RA)

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

Cada entidad que actúe como RA de Firmaprofesional 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 la presente CP.

- Los dispositivos de creación de firma a utilizar, de entre los que previamente Firmaprofesional haya homologado.

1.3.3 Suscriptores

El suscriptor del certificado será la entidad que aparece identificada en el Certificado.

El suscriptor del certificado de sello electrónico PSD2 será el proveedor del servicio de pago debidamente autorizado e inscrito en el registro público de la Autoridad Nacional Competente. El suscriptor será siempre una persona jurídica comprendida, al menos, en una de las categorías siguientes:

- Gestor de cuenta
- Proveedor de servicios de iniciación de pagos
- Proveedor de información sobre cuentas
- Emisor de instrumentos de pago basados en tarjetas.

1.3.3.1 Solicitante

Estos certificados podrán ser solicitados:

- Certificados de Sello de Órgano: cualquier persona autorizada por la Administración, Órgano o Entidad de derecho público.
- Certificados de Sello Empresarial: los administradores de la entidad, representantes legales y voluntarios con poder bastante a estos efectos o cualquier persona autorizada por los administradores, representantes legales o voluntarios.

1.3.4. Tercero que confía en los certificados

Los terceros que confíen en estos certificados deben tener presentes las limitaciones en su uso, establecidas en la CPS y en la presente CP.

Estos certificados 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

Estos certificados podrán usarse en los términos establecidos por la CPS, y lo establecido en la legislación vigente al respecto.

En concreto, el uso apropiado de cada tipo de certificado es el siguiente:

- **Certificados de Sello de Órgano:** Estos certificados pueden ser usados como mecanismo de identificación y autenticación en sistemas de firma electrónica para la actuación administrativa automatizada tal como establece el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **Certificados de Sello Empresarial:** Estos certificados pueden ser utilizados para autenticarse en sistemas de comunicaciones seguras, para la remisión de comunicaciones comerciales, para publicar informaciones en el sitio web de la empresa, etc. Estos certificados son válidos para su utilización en facturación electrónica y digitalización certificada y se ajustan a los requisitos que impone la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público han sido autorizados para su utilización en facturación electrónica y digitalización certificada por la Agencia Tributaria.
- **Certificados de Sello Electrónico para PSD2:** Estos certificados pueden utilizarse para que los proveedores de servicios de información sobre cuentas, los proveedores de servicios de iniciación de pagos y los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas puedan identificarse ante el proveedor de servicios de pago gestor de cuenta.

1.4.1.1. Periodo de validez de los certificados

El periodo de validez será el que se indique en el propio certificado, con un máximo siguiente:

Perfil	Otros dispositivos / Nivel Medio	DCCF / Nivel Alto
Sello de Órgano	Máximo 5 años	Máximo 5 años
Sello Empresarial	Máximo 5 años	–
Sello Electrónico para PSD2	Máximo 5 años	–

1.4.2 Usos prohibidos de los certificados

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Prácticas de Certificación, ni el uso que sea contrario a la normativa española y europea, a los convenios internacionales ratificados por el Estado español, a las costumbres, a la moral y al orden público.

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

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

3.1.3 Anonimato o uso de pseudónimos de los suscriptores

Sin estipulación.

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

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

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

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

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

Firmaprofesional únicamente aceptará las solicitudes que estén firmadas manual o electrónicamente por el solicitante del mismo y que cumplan con los requisitos establecidos para cada uno de los tipos de certificado.

4.1.1 Quién puede enviar una solicitud de certificado

Las solicitudes de estos certificados se realizan por administradores, representantes legales o voluntarios del Titular del Sello Electrónico debidamente acreditado y autorizado para ello o por aquellas personas autorizadas por dichos administradores, representantes legales o voluntarios.

4.1.2 Proceso de solicitud de certificados y responsabilidades

Los pasos a seguir para la obtención del certificado se detallan a continuación:

El solicitante deberá contactar directamente con Firmaprofesional, proporcionando toda la documentación necesaria para verificar la identidad de la persona jurídica.

En el caso solicitud de certificados de sello de órgano, Firmaprofesional verificará que:

- Existe una resolución de la Subsecretaría del Ministerio o titular del organismo público competente por la que se crea el Sello Electrónico y está publicada en la Sede Electrónica correspondiente, en el caso en que la ley lo exija.
- Los datos de la solicitud del certificado de Sello Electrónico coinciden con los datos publicados en la Resolución, en el caso en que la ley exija dicha resolución.

En caso de solicitar nivel ALTO, se deberá aportar evidencia de que la generación y custodia de claves se realiza en un dispositivo hardware criptográfico homologado por el Ministerio competente en materia de servicios de la sociedad de la información.

Firmaprofesional verificará la condición de representante legal o voluntario para la solicitud de los certificados de Sello Empresarial bien mediante una consulta telemática al Registro Mercantil o bien revisando la documentación notarial o legal aportada por el solicitante. El representante legal de la entidad podrá autorizar a una persona de la entidad como solicitante de los certificados de Sello Empresarial, y que será la persona responsable de su control y gestión, así como de su buen uso. Para ello, el solicitante deberá aportar un escrito del representante legal, donde se autorice expresamente al solicitante para la solicitud del certificado de sello empresarial, adjuntando copia del documento de identidad del autorizante y de sus poderes de representación, o bien en PDF firmado electrónicamente un su certificado de representante legal válido.

En los casos en que Firmaprofesional ya haya verificado previamente la identidad de la Persona Jurídica y del solicitante, no será necesario realizar verificaciones adicionales. En concreto:

- Si el solicitante dispone de un Certificado Corporativo de Representante Legal vigente emitido por Firmaprofesional.
- Si la Corporación actúa como RA de Firmaprofesional para la emisión de sus propios certificados.

En caso de solicitud de certificados de sello electrónico para PSD2, el proveedor del servicio de pago presentará la solicitud junto con el certificado de ser proveedor de servicios de pago

autorizado por la Autoridad Nacional Competente, junto con el número de autorización, el rol del proveedor del servicio de pago y el nombre de la Autoridad Nacional Competente del lugar donde esté registrado el proveedor de servicios de pago. La solicitud de emisión del certificado de sello electrónicos para PSD2 deberá estar firmada por una persona física que represente al proveedor de servicios de pago y que conste como tal en la Autoridad Nacional Competente.

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

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

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

4.3.1 Acciones de la CA durante la emisión del certificado

Cada Autoridad de Registro de Firmaprofesional tendrá acreditadas a una serie de personas para actuar como Operador de RA frente a Firmaprofesional. Los Operadores de RA habrán sido autorizados para realizar esta función y habrán sido previamente instruidos en la operativa de emisión de certificados.

Las fases de la tramitación son las siguientes:

1. Generación de claves

El Operador de RA validará la veracidad y exactitud de los datos del firmante y del solicitante.

En caso de los certificados de sello electrónico para PSD2, el operador de RA validará la información presentada por el proveedor de servicios de pago comparándola con la información disponible en el Registro Público de la Autoridad Nacional de Competencia.

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

El Operador de RA validará que el solicitante 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.

2. 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.

3. Entrega

Una vez se ha generado el certificado, y antes de que la RA pueda entregarlo al solicitante, 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 solicitante, ya sea entregando el DCCF portable, los mecanismos de autenticación y operación remota de firma electrónica o habilitando los mecanismos para su descarga y posterior uso.

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

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 por las partes que confían en los certificados

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

4.6. Renovación de certificados 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. Proceso 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 claves

4.7.1 Circunstancia para el cambio de clave del certificado

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

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.

4.7.3 Procesamiento de solicitudes de cambio de claves de certificados

En el caso de los certificados de Sello Empresarial, su renovación puede hacerse online siempre que la RA disponga del servicio y el suscriptor haya contratado la renovación. En este caso, el suscriptor recibirá una notificación de la RA por correo electrónico para iniciar la renovación a través de la página web de Firmaprofesional.

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.

La renovación de los certificados de Sello Electrónico para PSD2 implica necesariamente la comprobación de nuevo de todos los atributos del proveedor de servicios de pago, tal y como se hizo en la emisión inicial.

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

4.8.1. Circunstancia de la modificación del certificado

Sin estipulación.

4.8.2. Quién puede solicitar la modificación del certificado

Sin estipulación.

4.8.3. Tramitación de solicitudes de modificación de certificados

Sin estipulación.

4.8.4. Notificación de la emisión de un nuevo certificado al suscriptor

Sin estipulación.

4.8.5. Comportamiento que constituye la aceptación de un certificado modificado

Sin estipulación.

4.8.6. Publicación del certificado modificado por la AC

Sin estipulación.

4.8.7. Notificación de la expedición de certificados por la AC a otras entidades

Sin estipulación.

4.9 Revocación y suspensión de certificados

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 periodos 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
Certificado de Nivel Alto de Sello de Órgano emitido en un DCCF portable	1.3.6.1.4.1.13177.10.1.21.1
Certificado de Nivel Alto de Sello de Órgano emitido en un DCCF centralizado	1.3.6.1.4.1.13177.10.1.21.3

Certificado de Nivel Medio de Sello de Órgano emitido en otros dispositivos	1.3.6.1.4.1.13177.10.1.21.2
Certificado de Sello Empresarial y PSD2	1.3.6.1.4.1.13177.10.1.10.2
Certificado de Sello Empresarial en un DCCF centralizado	1.3.6.1.4.1.13177.10.1.10.3

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.

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.