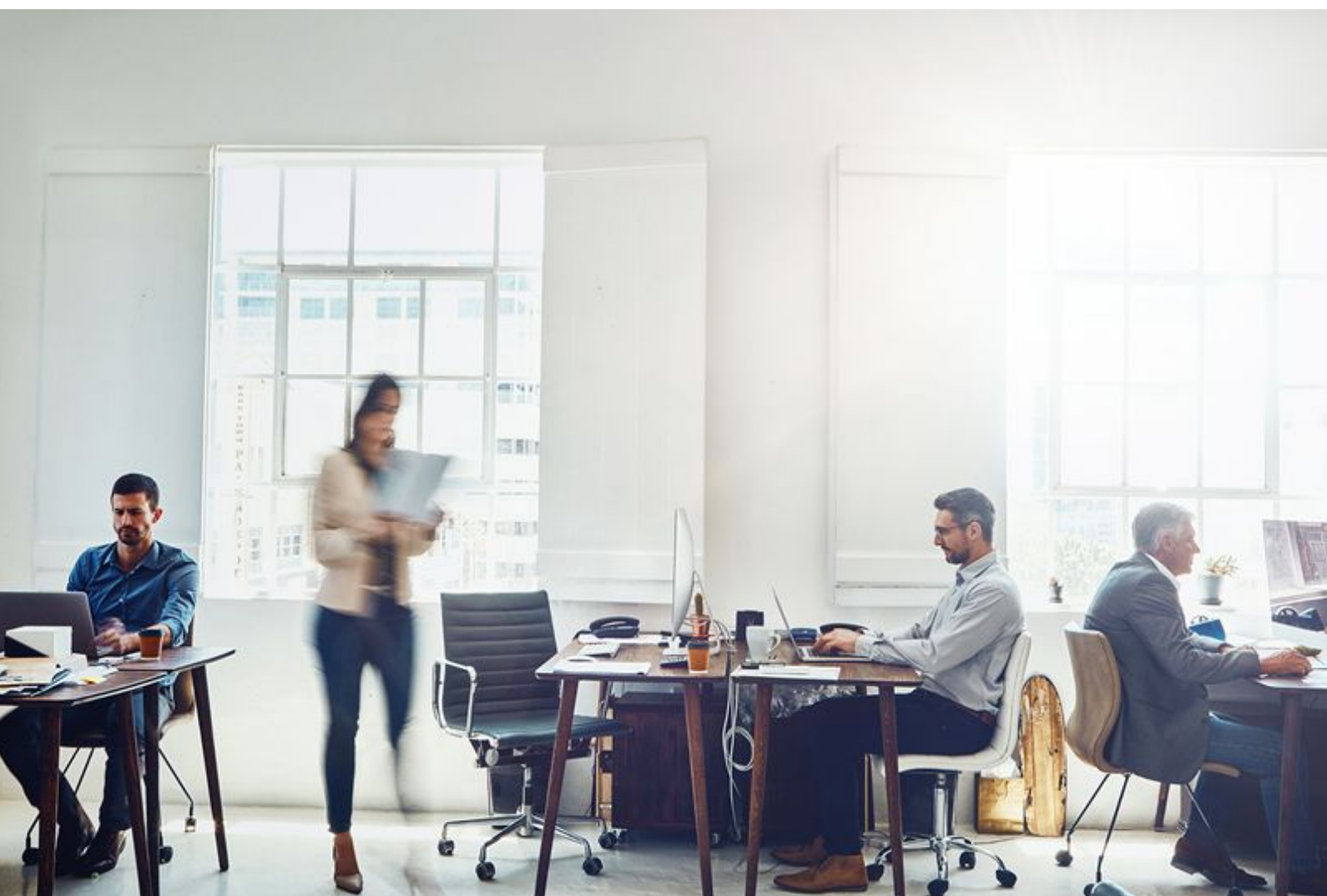


Política de Certificación

Certificados de Autenticación de sitios Web

Versión: 210217

Clasificación: Público



Histórico de versiones

Versión	Sección y cambios	Fecha de publicación
181221	<p>Elaboración de una nueva política certificados de autenticación de sitios web, que integra las anteriores políticas de certificado de sede electrónica y de servidor seguro SSL, que pueden ser consultadas en http://www.firmaprofesional.com/cps</p> <p>Además de la integración de las Políticas, se realizan las siguientes modificaciones:</p> <ul style="list-style-type: none"> ● "2.2. Autoridad de Registro (RA)": correcciones y aclaraciones. ● Campo SerialNumber marcado como opcional, dado que la misma información la contiene el campo OrganizationIdentifier. ● Procedimientos de verificación del dominio y la organización actualizados. ● Tratamiento de CAA explicado. ● Aclaración de los requisitos para la generación de claves de certificado de Sede Electrónica de nivel Alto 	21/12/2018
190121	<ul style="list-style-type: none"> ● "4.1.2.3.3. Verificación de la existencia operativa del solicitante": correcciones. ● "4.1.2.2.2. Verificación del control de dominio" de OV y "4.1.2.3.4. Verificación del control de dominio" de EV: homogeneización de los apartados. 	21/01/2019
190305	<ul style="list-style-type: none"> ● Reducida la validez máxima de los Certificados de Sede Electrónica, a 2 años. 	05/03/2019
190507	<ul style="list-style-type: none"> ● "3.3. Certificados multidominio": correcciones. ● Añadida verificación de control de los dominios de certificados SSL multidominio 	07/05/2019
190612	<ul style="list-style-type: none"> ● Inclusión de certificados de autenticación web para servicios de pago basados en la Directiva de servicios de pago 2015/2366 (PSD2) 	12/06/2019
190806	<ul style="list-style-type: none"> ● Reestructuración de puntos del histórico de versiones ● "4.1.2.2.2. Verificación del control del nombre de dominio": indicado que el código aleatorio se envía al contacto del dominio. 	06/08/2019

	<ul style="list-style-type: none"> • “4.2. Revocación y suspensión de certificados”: incluida la suspensión para explicitar que no está permitida por esta política. 	
200205	<ul style="list-style-type: none"> • “4.1.1.4. Solicitud para certificados de PSD2”, reformulado el procedimiento de solicitud para homogeneizarlo con el de EV. • “4.1.2.1. Aceptación de la solicitud para certificados de Sede Electrónica”, actualizado apartado eliminando partes que no aplican. • Adaptación de la Política a los requerimientos de la versión 2.7 de la Política de Mozilla Root Store. • “4.1.2.2.1. Verificación de la identidad del solicitante”. Eliminación de referencias a secciones obsoletas 	05/02/2020
200806	<ul style="list-style-type: none"> • Ampliación de los mecanismos de Verificación de la existencia legal e identidad del solicitante en la sección 4.1.2.3.1, añadiendo “Apoderamiento o Representación legal.” • Incorporación del subapartado 4.1.2.1.1 Verificación del control del nombre de dominio. 	06/08/2020
200901	<ul style="list-style-type: none"> • Reducida la validez máxima de los Certificados a 1 año. 	01/09/2020
201001	<ul style="list-style-type: none"> • Incorporación en sección 3.2 referencia a la tabla de registro de fuentes de verificación 	01/10/2020
210217	<ul style="list-style-type: none"> • Adaptación a la nueva Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza. • Adaptación a la RFC3647 	17/02/2021

Índice

1. Introducción	16
1.1. Resumen	16
1.2. Identificación del Documento	18
1.3. Entidades Participantes	18
1.3.1 Autoridades de Certificación (CA)	18
1.3.2 Autoridad de Registro (RA)	18
1.3.3 Suscriptores	19
1.3.3.1 Solicitante	19
1.3.3.2 Roles intervinientes	20
1.3.4 Terceros que confían en los certificados	21
1.3.5 Otros participantes	21
1.4 Uso de Certificados	22
1.4.1 Usos apropiados de los certificados	22
1.4.1.1 Periodo de validez de los certificados	22
1.4.1.2 Certificados extended validation (EV)	22
1.4.1.3 Certificados multidominio	22
1.4.1.4 Nombres de dominio	23
1.4.2 Usos prohibidos de los certificados	23
1.4.2.1 Notificación de usos no autorizados, quejas o sugerencias	24
1.5 Administración de Políticas	24
1.5.1 Organización que administra el documento	24
1.5.2 Persona de contacto	24
1.5.3 Persona que determina la idoneidad de la CP para la póliza	24
1.5.4 Procedimiento de aprobación de la CP	25
1.6 Definiciones y siglas	25

2. Repositorios y Publicación de Información	25
3. Identificación y Autenticación	26
3.1 Nombrar	26
3.1.1 Tipos de nombres	26
3.1.2 Necesidad de que los nombres sean significativos	26
3.1.3 Anonimato o seudonimato de los suscriptores	26
3.1.4 Reglas para interpretar varias formas de nombres	26
3.1.5 Unicidad de los nombres	26
3.1.6 Reconocimiento, autenticación y función de las marcas	27
3.2 Validación de identidad inicial	27
3.2.1 Método de prueba de posesión de clave privada	29
3.2.2 Autenticación de la identidad de la organización e identidad de dominio	29
3.2.2.1 Validación de dominio	29
3.2.3 Autenticación de la identidad individual	30
3.2.4 Información de abonado no verificada	30
3.2.5 Validación de autoridad	31
3.2.6 Criterios de interoperación	31
3.3 Identificación y autenticación para solicitudes de renovación de claves	31
3.3.1 Identificación y autenticación para el cambio de clave de rutina	31
3.3.1.1 Renovación de certificados online	31
3.3.1.2. Renovación de certificados con personación	31
4. Requisitos operativos del ciclo de vida del certificado	32
4.1. Solicitud del certificado	32
4.1.1. Quién puede enviar una solicitud de certificado	32
4.1.1.1. Solicitud para certificados de Sede Electrónica	32
4.1.1.2. Solicitud para certificados OV	32
4.1.1.3. Solicitud para certificados EV	33
4.1.1.4. Solicitud para certificados de PSD2	34

4.1.2. Proceso de solicitud de certificados y responsabilidades	34
4.2 Tramitación de las solicitudes de certificados	35
4.2.1 Realización de las funciones de identificación y autenticación	35
4.2.2 Aprobación o denegación de las solicitudes de certificados	35
4.2.3 Tiempo de tramitación de las solicitudes de certificado	36
4.3 Emisión de certificados	36
4.3.1 Acciones de la CA durante la emisión del certificado	36
4.3.2 Notificación al suscriptor por parte de la CA de la emisión del certificado y entrega	36
4.4. Aceptación del certificado	37
4.4.1 Forma en la que se acepta el certificado	37
4.4.1.1 Aceptación de la solicitud para certificados de Sede Electrónica	37
4.4.1.1.1 Verificación del control del nombre de dominio	37
4.4.1.2. Aceptación de la solicitud para certificados OV	37
4.4.1.3. Aceptación de la solicitud para certificados EV	38
4.4.1.3.1. Verificación de la existencia legal e identidad del solicitante	39
4.4.1.3.2. Verificación de la ubicación geográfica en la que el solicitante desarrolla su negocio	41
4.4.1.3.3. Verificación de la existencia operativa del solicitante	41
4.4.1.3.4. Verificación del control del nombre de dominio	41
4.4.1.3.5. Verificación del nombre, cargo y autoridad del firmante del contrato de suscriptor y de aprobador del certificado	42
4.4.1.3.6. Verificación de la firma del contrato de suscriptor.	42
4.4.1.3.7. Verificación de la aprobación para la emisión de un certificado SSL EV.	43
4.4.1.4. Aceptación de la solicitud para certificados de PSD2	43
4.4.2 Publicación del certificado por la CA	43
4.4.3 Notificación de la emisión del certificado por parte de la CA a otras entidades	43
4.5 Uso de las claves y el certificado	44
4.5.1 Uso de la clave privada y del certificado por el suscriptor	44

4.5.2	Uso de la clave pública y del certificado por los terceros que confían en los certificados	44
4.6	Renovación del certificado sin cambio de claves	44
4.6.1	Circunstancia para la renovación del certificado	44
4.6.2	Quién puede solicitar la renovación	44
4.6.3	Proceso de solicitudes de renovación de certificados	44
4.6.4	Notificación al suscriptor de la emisión de un nuevo certificado	44
4.6.5	Conducta que constituye la aceptación de un certificado de renovación	45
4.6.6	Publicación del certificado de renovación por parte de la CA	45
4.6.7	Notificación de la emisión del certificado por parte de la CA a otras entidades	45
4.7	Renovación del certificado con cambio de claves	45
4.7.1	Circunstancias para la renovación online con cambio de claves	45
4.7.2	Quién puede pedir la renovación online de un certificado	45
4.7.3	Tramitación de las peticiones de renovación online	45
4.7.4	Notificación de la emisión del certificado renovado	45
4.7.5	Forma de aceptación del certificado renovado	46
4.7.6	Publicación del certificado renovado	46
4.7.7	Notificación de la emisión del certificado por parte de la CA a otras entidades	46
4.8	Modificación de certificados	46
4.8.1	Circunstancia de la modificación de certificado	46
4.8.2	Quién puede solicitar la modificación del certificado	46
4.8.3	Tramitación de solicitudes de modificación de certificados	46
4.8.4	Notificación de la emisión de un nuevo certificado al suscriptor	46
4.8.5	Comportamiento que constituye la aceptación de un certificado modificado	47
4.8.6	Publicación del certificado modificado por la AC	47
4.8.7	Notificación de la expedición de certificados por la AC a otras entidades	47
4.9	Revocación y suspensión de certificados	47
4.9.1	Circunstancias para la revocación	47

4.9.2	Quién puede solicitar la revocación	47
4.9.3	Procedimientos de solicitud de revocación	47
4.9.4	Periodo de gracia de la solicitud de revocación	48
4.9.5	Plazo en el que la CA debe resolver la solicitud de revocación	48
4.9.6	Obligación de verificación de las revocaciones por los terceros	48
4.9.7	Frecuencia de emisión de CRLs	48
4.9.8	Tiempo máximo entre la generación y la publicación de las CRLs	48
4.9.9	Disponibilidad del sistema en línea de verificación del estado de los certificados	48
4.9.10	Requisitos de comprobación de revocación en línea	48
4.9.11	Otras formas de anuncios de revocación disponibles	49
4.9.12	Necesidades especiales en relación con el compromiso de clave	49
4.9.13	Circunstancias para la suspensión	49
4.9.14	Quién puede solicitar la suspensión	49
4.9.15	Procedimiento de solicitud de suspensión	49
4.9.16	Límites del periodo de suspensión.	49
4.10	Servicios de información del estado de certificados	50
4.10.1	Características operativas	50
4.10.2	Disponibilidad del servicio	50
4.10.3	Características adicionales	50
4.11	Finalización de la suscripción	50
4.12	Custodia y recuperación de claves	50
4.12.1	Política y prácticas fundamentales de custodia y recuperación	50
4.12.2	Política y prácticas de encapsulamiento y recuperación de claves de sesión	50
5.	Controles de seguridad física, instalaciones, gestión y operacionales	51
5.1	Controles físicos	51
5.1.1.	Ubicación física y construcción	51
5.1.2.	Acceso físico	51

5.1.3. Alimentación eléctrica y aire acondicionado	51
5.1.4 Exposición al agua	51
5.1.5. Protección y prevención de incendios	51
5.1.6. Sistema de almacenamiento	52
5.1.7 Eliminación de los soportes de información	52
5.1.8. Copias de seguridad fuera de las instalaciones	52
5.2 Controles de procedimiento	52
5.2.1. Roles de los responsables	52
5.2.2. Número de personas requeridas por tarea	52
5.2.3. Identificación y autenticación por rol	52
5.2.4. Roles que requieren segregación de funciones	53
5.3 Controles de personal	53
5.3.1. Requisitos relativos a la calificación, conocimiento y experiencia profesionales	53
5.3.2. Procedimientos de comprobación de antecedentes	53
5.3.3. Requerimientos de formación	53
5.3.4. Requerimientos y frecuencia de actualización de la formación	53
5.3.5. Frecuencia y secuencia de rotación de tareas	53
5.3.6. Sanciones por actuaciones no autorizadas	54
5.3.7. Requisitos de contratación de terceros	54
5.3.8. Documentación proporcionada al personal	54
5.4 Procedimientos de auditoría de seguridad	54
5.4.1. Tipos de eventos registrados	54
5.4.2. Frecuencia de procesado de registros de auditoría	54
5.4.3. Periodo de conservación de los registros de auditoría	54
5.4.4. Protección de los registros de auditoría	55
5.4.5. Procedimientos de respaldo de los registros de auditoría	55
5.4.6. Sistema de recogida de información de auditoría	55
5.4.7. Notificación al sujeto causante del evento	55

5.4.8. Análisis de vulnerabilidades	55
5.5 Archivo de registros	55
5.5.1. Tipo de eventos archivos	55
5.5.2. Periodo de conservación de registros	56
5.5.3. Protección del archivo	56
5.5.4 Procedimientos de copia de seguridad del archivo	56
5.5.5 Requerimientos para el sellado de tiempo de los registros	56
5.5.6. Sistema de archivo de información de auditoría	56
5.5.7. Procedimientos para obtener y verificar información archivada	56
5.6 Cambio de claves de la CA	57
5.6.1. CA Raíz	57
5.6.2. CA Subordinada	57
5.7 Plan de recuperación de desastres	57
5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades	57
5.7.2. Alteración de los recursos hardware, software y/o datos	57
5.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una Autoridad de Certificación o de la suite criptográfica	57
5.7.4. Continuidad de Negocio después de un desastre	57
5.8 Cese de actividad	58
5.8.1. Autoridad de Certificación	58
5.8.2. Autoridad de Registro	58
6. Controles de seguridad técnica	58
6.1 Generación e instalación del par de claves	58
6.1.1 Generación del par de claves	58
6.1.2 Entrega de la clave privada al firmante	58
6.1.3 Entrega de la clave pública al emisor del certificado	59
6.1.4 Entrega de la clave pública de la CA a los terceros que confían en los certificados	59
6.1.5. Tamaño de las claves	59

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad	59
6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509v3)	59
6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos	59
6.2.1 Estándares para los módulos criptográficos	59
6.2.2 Control multipersona (k de n) de la clave privada	60
6.2.3 Custodia de la clave privada	60
6.2.4. Copia de seguridad de la clave privada	60
6.2.5. Archivo de la clave Privada	60
6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico	60
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico	60
6.2.8. Método de activación de la clave privada	60
6.2.9. Método de desactivación de la clave privada	61
6.2.10 Método de destrucción de la clave privada	61
6.2.11 Clasificación de los módulos criptográficos	61
6.3. Otros aspectos de la gestión del par de claves	61
6.3.1 Archivo de la clave pública	61
6.3.2 Periodos de operativos de los certificados y periodo de uso para el par de claves	61
6.4 Datos de activación	61
6.4.1 Generación e instalación de los datos de activación	61
6.4.2 Protección de los datos de activación	62
6.4.3 Otros aspectos de los datos de activación	62
6.5 Controles de seguridad informática	62
6.5.1 Requerimientos técnicos de seguridad específicos	62
6.5.2. Evaluación de la seguridad informática	62
6.6. Controles de seguridad del ciclo de vida	62
6.6.1 Controles de desarrollo de sistemas	62
6.6.2 Controles de gestión d seguridad	62

6.6.3 Gestión del ciclo de vida del hardware criptográfico	63
6.7 Controles de seguridad en la red	63
6.8. Fuente de tiempo	63
7. Perfiles de los certificados, CRL y OCSP	63
7.1 Perfil de los certificados	63
7.1.1 Número de versión	64
7.1.2. Extensiones de los certificados	64
7.1.3. Identificadores de objeto (OID) de los algoritmos utilizados	64
7.1.4. Formatos de nombres	64
7.1.5. Restricciones de los nombres	64
7.1.6. Identificador de objeto (OID) de la Política	64
7.1.7 Extensión del uso de las restricciones de política	65
7.1.8 Sintaxis y semántica de los “PolicyQualifier”	65
7.1.9 Tratamiento semántico para la extensión “Certificate Policy”	65
7.2 Perfil de CRL	65
7.2.1 Número de versión	65
7.2.2 CRL y extensiones	65
7.3 Perfil de OCSP	65
7.3.2 OCSP y extensiones	66
8. Auditorías de cumplimiento y otros controles	66
8.1. Frecuencia de las auditorías	66
8.2. Cualificación del auditor	66
8.3 Relación entre el auditor y la autoridad auditada	66
8.4 Aspectos cubiertos por los controles	66
8.4.1 Auditorías en las Autoridades de Registro	66
8.5 Acciones a emprender como resultado de la detección de incidencias	66
8.6 Comunicación de resultados	67
9. Otras cuestiones legales y de actividad	67

9.1 Tarifas	67
9.1.1 Tarifas de emisión de certificado o renovación	67
9.1.2 Tarifas de acceso a los certificados	67
9.1.3 Tarifas de acceso a la información de estado o revocación	67
9.1.4 Tarifas de otros servicios	67
9.1.5 Política de reembolso	68
9.2 Responsabilidades económicas	68
9.2.1 Cobertura de seguro	68
9.2.2 Otros activos	68
9.2.3 Seguro o cobertura de garantía para las entidades finales	68
9.3 Confidencialidad de la información	68
9.3.1 Ámbito de la información confidencial	68
9.3.2 Información no confidencial	68
9.3.3 Responsabilidad en la protección de información confidencial	69
9.4 Protección de la información personal	69
9.4.1 Política de protección de datos de carácter personal	69
9.4.2 Información tratada como privada	69
9.4.3 Información no calificada como privada	69
9.4.4. Responsabilidad de la protección de los datos de carácter personal	69
9.4.5 Comunicación y consentimiento para usar datos de carácter personal	69
9.4.6 Revelación en el marco de un proceso judicial	70
9.4.7 Otras circunstancias de publicación de información	70
9.5 Derechos de propiedad intelectual	70
9.6 Obligaciones	70
9.6.1 Obligaciones de la CA	70
9.6.2 Obligaciones de la RA	70
9.6.3 Obligaciones de los solicitantes	70
9.6.4 Obligaciones de los terceros que confían en los certificados	71

9.6.5 Obligaciones de otros participantes	71
9.7 Exención de garantía	71
9.8 Responsabilidades	71
9.8.1 Responsabilidades de la Autoridad de Certificación	71
9.8.2 Responsabilidades de la Autoridad de Registro	71
9.8.3 Responsabilidades del suscriptor	71
9.8.4 Delimitación de responsabilidades	71
9.9 Indemnizaciones	72
9.9.1 Alcance de la cobertura	72
9.9.2 Cobertura de seguro y otras garantías para los terceros aceptantes	72
9.9.3 Limitaciones de pérdidas	72
9.10 Periodo de validez	72
9.10.1 Plazo	72
9.10.2 Sustitución y derogación de la CPS	72
9.10.3 Efectos de la finalización	72
9.11 Notificaciones individuales y comunicación con los participantes	73
9.12 Cambios en las especificaciones	73
9.12.1 Procedimiento para los cambios	73
9.12.2 Periodo y procedimiento de notificación	73
9.12.3 Circunstancias en las que el OID debe ser cambiado	73
9.13 Reclamaciones y resolución de conflictos	74
9.14 Normativa aplicable	74
9.15 Cumplimiento de la normativa aplicable	74
9.16 Estipulaciones diversas	74
9.16.1 Cláusula de aceptación completa	74
9.16.2 Independencia	74
9.16.3 Resolución por la vía judicial	74
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)	74

9.16.5 Fuerza mayor	75
9.17 Otras provisiones	75

1. Introducción

1.1. Resumen

Los certificados de autenticación de sitios web son certificados expedidos a organizaciones para servidores web, y garantizan a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda la existencia del sitio web. Como se establece en el Considerando 67 del Reglamento UE 910/2014 del Parlamento y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, estos certificados contribuyen a crear confianza y fe en la realización de operaciones mercantiles y administrativas en línea, dado que los usuarios se fiarán de un sitio web que haya sido autenticado.

En la actualidad, Firmaprofesional emite cuatro tipos de Certificados de Autenticación de sitios Web:

- **Certificados de Sede**
 - Son certificados expedidos a Administraciones Públicas, de acuerdo con las indicaciones del artículo 38 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
 - Son certificados cualificados porque cumplen los requisitos establecidos en el anexo IV del Reglamento UE 910/2014.
 - Estos certificados se adhieren a las definiciones de los niveles de aseguramiento alto y medio y a los perfiles de certificados establecidos en el punto 8 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.
- **Certificados SSL Organization Validation (OV):**
 - Garantizan que un determinado dominio ha sido registrado a nombre de la organización identificada en el certificado y que la comunicación entre el navegador del cliente y el servidor de páginas es confidencial debido al empleo del protocolo SSL.
 - Se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento “*Baseline Requirements for the Issuance and Management of*

Publicly Trusted Certificates,” vigente en el momento de la publicación de la presente política.

- **Certificados SSL *Extended Validation* (EV):**

- Son certificados emitidos a servidores de páginas web expedido de acuerdo con un conjunto específico de criterios de verificación de la identidad de la organización identificada en el certificado.
- Un certificado SSL EV permite a los navegadores que se conectan a este servicio, mostrar un nivel de seguridad adicional.
- Se ajustan a los requerimientos del CA/Browser Forum establecidos en el documento “*Guidelines for the issuance and management of Extended Validation certificates*” vigente en el momento de la publicación de la presente política.
- Son certificados cualificados porque cumplen los requisitos establecidos en el anexo IV del Reglamento UE 910/2014.

- **Certificados de autenticación web para PSD2**

- Son certificados de autenticación web para servicios de pago.
- Estos certificados se emiten únicamente a proveedores de servicios de pago autorizados por la Autoridad Nacional Competente, de acuerdo con la Directiva UE 2015/2366, el Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE (Directiva PSD2).
- Se ajustan a los requerimientos de la ETSI TS 119 495.

En el presente documento se exponen las condiciones particulares referentes a estos 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.

En el caso de cualquier incompatibilidad entre este documento y los requisitos publicados por el CA/Browser Forum, los requisitos tienen prioridad sobre este documento.

1.2. Identificación del Documento

Nombre:	Política de Certificación para Certificados de Autenticación de sitios Web
Versión:	210217
Descripción:	Política de Certificación para Certificados de Autenticación de sitios Web
Fecha de Emisión:	17/02/2021
OIDs	1.3.6.1.4.1.13177.10.1.20.1 Sede Electrónica Nivel Alto 1.3.6.1.4.1.13177.10.1.20.2 Sede Electrónica Nivel Medio 1.3.6.1.4.1.13177.10.1.3.1 SSL OV 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Cualificado /PSD2
Localización	http://www.firmaprofesional.com/cps

Esta Política de Certificación agrupa las siguiente Políticas, que quedan derogadas con la publicación de ésta:

- Política de Certificación de Certificados de Sede Electrónica (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 de Servidor Web Seguro (Versión 180719). 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)

Desde la fecha de publicación de la presente Política, todos los certificados de Autenticación Web son emitidos por la CA Subordinada "AC Firmaprofesional - INFRAESTRUCTURA".

1.3.2 Autoridad de Registro (RA)

La gestión de las solicitudes de los certificados será realizada por Firmaprofesional o por un Intermediario autorizado.

La gestión de las emisiones únicamente podrá ser realizada por Firmaprofesional.

1.3.3 Suscriptores

El suscriptor del certificado de autenticación de sitios web será la organización que aparece como "Registrante" ("Registrant") en el registro oficial del dominio, o la Administración, Órgano o Entidad de Derecho público identificada en el certificado.

El suscriptor del certificado de autenticación web 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

Es la persona física o jurídica que solicita el certificado.

En general, podrá realizar la solicitud de estos certificados en nombre de una organización la persona que aparezca como "Contacto Administrativo" en el registro oficial del dominio.

En el caso de certificados de Sede Electrónica, podrán solicitarlos los administradores, representantes legales y voluntarios de las Corporaciones Públicas, con poder bastante a estos efectos.

En el caso de certificados de autenticación web para PSD2, el solicitante será el representante legal del proveedor de servicios de pago, que conste como tal en el Banco de España (para proveedores españoles) o Autoridad Nacional Competente.

1.3.3.2 Roles intervinientes

Siguiendo lo estipulado en la versión vigente del documento "*Guidelines For The Issuance And Management Of Extended Validation Certificates*", emitido por CA/Browser Forum, se establecen una serie de roles que pueden desempeñar diferentes personas relacionadas con el solicitante de un certificado SSL EV.

Estos roles son los siguientes:

1. **El petionario de certificados:**

La solicitud de un certificado SSL EV debe ser realizada por un petionario autorizado por el solicitante. Un petionario puede ser el mismo solicitante (si este es una persona física), un empleado del solicitante, un agente autorizado que está autorizado por el solicitante para representarle, un empleado de una tercera parte (por ejemplo, un ISP o una empresa de hosting de sitios web). El petionario cumple la siguiente función:

- a. Completar y enviar las solicitudes de certificados.

2. **El aprobador de certificados:**

La solicitud de un certificado SSL EV debe ser aprobada por un aprobador autorizado por el solicitante. Un aprobador puede ser el mismo solicitante (si este es una persona física), un empleado del solicitante, un agente autorizado por el solicitante para representarle. El aprobador puede cumplir las siguientes funciones:

- a. Actuar como un petionario, completando y enviando solicitudes de certificados.
- b. Autorizar a otros empleados o a terceras partes para actuar como petionarios.
- c. Aprobar las solicitudes de certificados enviadas por petionarios.

3. **El firmante del contrato de suscriptor:**

Para solicitar un certificado SSL EV se debe firmar un contrato de suscriptor por un firmante autorizado para ello. Un firmante de contrato es una persona física que

puede ser el mismo solicitante, un empleado del solicitante o un agente autorizado por el solicitante para representarlo, que dispone de la autoridad para firmar el contrato de suscriptor en representación del solicitante. El firmante cumple la siguiente función:

- a. Firmar el contrato del suscriptor.

4. **El representante del solicitante:**

En el caso de que la CA y el suscriptor sean compañías filiales, los términos de uso aplicables a la solicitud de certificados SSL EV deben ser conocidos y aceptados por un representante autorizado del solicitante. Un representante del solicitante es una persona física que puede ser el mismo solicitante, o un agente autorizado por el solicitante para representarle, y tiene la autoridad de confirmar el conocimiento y la aceptación de los términos de uso en representación del solicitante.

1.3.4 Terceros que confían en los certificados

Estos certificados están reconocidos por Microsoft en todas sus aplicaciones, incluyendo Internet Explorer, por la Fundación Mozilla, incluyendo el navegador Firefox y por Apple, incluyendo el navegador Safari. La plataforma @firma, la Plataforma de validación y firma electrónica del Gobierno de España, admite y valida los certificados de Sede Electrónica, nivel medio y alto y los certificados de SSL OV.

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

1.3.5 Otros participantes

Sin estipulación.

1.4 Uso de Certificados

1.4.1 Usos apropiados de los certificados

Los Certificados de Autenticación de sitios Web pueden ser utilizados para autenticar la identidad de un servidor o de una Sede Electrónica mediante el protocolo SSL (o TLS) y establecer luego un canal de transmisión seguro entre el servidor o la Sede y el usuario del servicio.

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 de 1 (un) año para todos los certificados emitidos bajo la presente Política.

1.4.1.2 Certificados extended validation (EV)

Los Certificados de Servidor Web SSL EV permiten a los navegadores que se conectan a este servicio mostrar un nivel de seguridad adicional al de los Certificados de Servidor Web SSL OV.

Para ello se emiten de acuerdo con un conjunto específico de criterios de verificación de la identidad de la organización identificada en el certificado muy riguroso. Estos criterios requieren una verificación exhaustiva de la identidad de la organización solicitante y de la persona que hace efectiva la solicitud. Mediante la firma electrónica de la solicitud de un Certificado de Servidor Web SSL EV realizada con un Certificado Corporativo de Representante Legal emitido por Firmaprofesional se cubre gran parte de estos requisitos.

La lista de Agencias Incorporadoras o Agencias de Registro se publica en el repositorio del sitio web de Firmaprofesional (www.firmaprofesional.com), en la sección "Fuentes de Verificación".

1.4.1.3 Certificados multidominio

Los Certificados de Servidor Web Multidominio permiten validar diferentes URLs del mismo dominio con el mismo certificado.

Una forma de realizarlo es utilizando “Caracteres Wildcards” para las URLs tal como se definen en el estándar RFC 2818 “HTTP Over TLS”.

Según este estándar, se permite utilizar el carácter “asterisco” como comodín dentro de una URL. De este modo, un certificado con la URL “*.dominio.com” podrá ser utilizado para cualquier subdominio, como “subdominio1.dominio.com”, “subdominio2.dominio.com”, “www.dominio.com”, etc...

El uso de “wildcards” en Certificados de Servidor Web SSL está soportado por los principales navegadores de Internet y resulta muy útil cuando se disponen de muchos subdominios del mismo dominio de Internet y se desea utilizar un único certificado para todos ellos.

Únicamente se permite emitir certificados wildcard para certificados de servidor SSL OV.

Los Certificados de Servidor Web SSL EV y los certificados de Sede Electrónica no pueden ser wildcard. Sin embargo, tanto los certificados de Servidor Web SSL OV como EV y los certificados de Sede Electrónica podrán ser multidominio, protegiendo con el certificado varios nombres de host a través de múltiples dominios.

1.4.1.4 Nombres de dominio

No se permite la emisión certificados a direcciones IP o Nombres de Dominio internos, privados o reservados.

El uso de nombres de dominio internacionalizados (IDN por sus siglas en inglés) no está permitido bajo esta política de certificado. Esta medida previene ataques de spoofing homográfico.

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.

No se permite el uso de este tipo de certificado para la firma electrónica de documentos. Firmaprofesional dispone de otras políticas de certificado apropiadas para tal fin.

No se permite la utilización distinta de lo establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público para los certificados de Sede Electrónica.

1.4.2.1 Notificación de usos no autorizados, quejas o sugerencias

En caso de detectar un uso no autorizado de los certificados o tener alguna queja o sugerencia, éstas se deben hacer llegar a Firmaprofesional mediante correo electrónico a la dirección sopORTE@firmaprofesional.com, indicando en el asunto si se trata de un “Uso no autorizado”, una “Queja” o una “Sugerencia” y aportando en el cuerpo del correo y mediante archivos adjuntos la información necesaria para que Firmaprofesional pueda validar la veracidad de las afirmaciones realizadas

1.5 Administración de Políticas

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

1.5.1 Organización que administra el documento

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

1.5.2 Persona de contacto

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

1.5.4 Procedimiento de aprobación de la CP

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

1.6 Definiciones y siglas

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

2. Repositorios y Publicación de Información

2.1 Repositorios

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

2.2 Publicación de información de certificación

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

2.3 Hora o frecuencia de publicación

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

2.4 Control de acceso a los repositorios

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

3. Identificación y Autenticación

3.1 Nombrar

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

3.1.1 Tipos de nombres

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

3.1.2 Necesidad de que los nombres sean significativos

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

3.1.3 Anonimato o seudonimato de los suscriptores

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

3.1.4 Reglas para interpretar varias formas de nombres

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

3.1.5 Unicidad de los nombres

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

3.1.6 Reconocimiento, autenticación y función de las marcas

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

3.2 Validación de identidad inicial

La lista de Agencias Incorporadoras o Agencias de Registro se publica en el repositorio del sitio web de Firmaprofesional (www.firmaprofesional.com), en la sección "Fuentes de Verificación".

Se siguen los siguientes pasos para verificar la información del certificado:

1. **Si el solicitante es una organización (persona jurídica):** se verifica su existencia, nombre, dirección y país de la organización, utilizando uno de los siguientes medios:
 - a. Consulta al registro oficial dependiendo del tipo de organización de que se trate. Por ejemplo, para empresas, se realizará la consulta al Registro Mercantil. En el caso de entidades públicas, se realizará una consulta a un registro de entidades públicas.

También se admite un documento firmado emitido por un registro oficial 825 días antes de la emisión del certificado.
 - b. Consulta en una base de datos de un tercero periódicamente actualizada y que es considerada como fuente de datos confiable. Como fuente de datos confiable se entiende una base de datos usada para verificar información acerca de la identidad de organizaciones, reconocida entre las empresas comerciales y administraciones públicas como fuente confiable y creada por una tercera parte, que no sea el mismo solicitante.

También es válido un documento o informe emitido por una fuente confiable, como por ejemplo, Legal Entity Identifier (LEI).

- c. Una declaración escrita por un funcionario público, notario o despacho de abogados.

Si el solicitante desea incorporar en el certificado la información de una **marca registrada o de un nombre comercial**, entonces se verifica que tiene derecho a usar la marca o el nombre usando uno los siguientes medios:

- a. Certificado emitido por una entidad gubernamental o consulta a un registro oficial, en el que se demuestre que el solicitante tiene derecho a utilizar la marca o el nombre que aparecerá en el certificado. Por ejemplo, en España se realizará una búsqueda en el registro Web de la Oficina Española de Patentes y Marcas. También, serviría que el solicitante aporte un certificado de esta misma entidad.
- b. Consulta en una base de datos de un tercero periódicamente actualizada y que es considerada como fuente de datos confiable. Como fuente de datos confiable se entiende una base de datos usada para verificar que una organización posee el derecho a usar una marca o un nombre comercial, y que es reconocida entre las empresas comerciales y administraciones públicas como fuente confiable y creada por una tercera parte, que no sea el mismo solicitante.
También es válido un documento o informe emitido por una fuente confiable.
- c. Una declaración escrita por un funcionario público, notario o despacho de abogados, acompañada de documentación que acredite que el solicitante tiene derecho a usar el nombre comercial o la marca.

2. **Si el solicitante es una persona física:** se verifica el nombre, su dirección y país, utilizando uno de los siguientes medios:
 - a. Fotocopia del DNI, pasaporte o carné de conducir, en la que aparezca una fotografía en la que se pueda discernir la cara del solicitante. Este medio

servirá para verificar el nombre y la dirección del solicitante.

- b. Si la ubicación que se desea incluir en el certificado no es la misma que aparece en el DNI, pasaporte o carné de conducir, el solicitante puede aportar una factura de agua o luz o un extracto bancario, en el que se asocie al solicitante con la ubicación que se desea incluir en el certificado

3.2.1 Método de prueba de posesión de clave privada

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

3.2.2.1 Validación de dominio

Firmaprofesional verifica, antes de la emisión del certificado SSL, que el solicitante tiene control sobre el dominio para el cual solicita el certificado; si la solicitud se realiza para un certificado SSL multidominio, Firmaprofesional verifica que todos los dominios que se añaden al SAN (Subject Alternative Name) pertenecen a la misma organización. La verificación se realizará utilizando al menos uno de los siguientes métodos:

1. Se envía al contacto del dominio un código único y aleatorio por correo electrónico, fax, mensaje SMS o carta por correo postal. Cualquier persona de la organización solicitante puede contestar por cualquiera de estos medios, indicando el código aleatorio. Lo más frecuente será que responda por E-Mail.
Para enviar el código aleatorio, Firmaprofesional utilizará la dirección de correo electrónico, el número de fax, el número de teléfono móvil o la dirección de correo

postal que aparece en el resultado de la búsqueda realizada en el servicio Whois.

2. Se realiza una llamada al contacto administrativo o técnico del nombre de dominio, que aparece en la consulta realizada al servicio Whois correspondiente. En la llamada se confirma que el solicitante ha realizado la petición de un certificado para el nombre de dominio en cuestión. La llamada se realiza al número de teléfono que muestra el resultado de la búsqueda al servicio Whois. La llamada es grabada y almacenada por Firmaprofesional.
3. Se envía un correo electrónico a una o más de las siguientes direcciones "admin", "administrator", "webmaster", "hostmaster" o "postmaster", seguido por el símbolo "@" y el nombre de dominio para el cual se solicita el certificado SSL. El correo electrónico enviado por Firmaprofesional incluye un código aleatorio y único. Cualquier persona de la organización solicitante debe responder el correo electrónico indicando el código aleatorio.
4. El solicitante realiza un cambio en el registro DNS del dominio para el que peticona el certificado SSL. Firmaprofesional le indica un código aleatorio y único. El solicitante debe añadir el código aleatorio en un campo CNAME, TXT o CAA, en su registro DNS. Una vez realizado el cambio por parte del solicitante, Firmaprofesional lo verifica.

3.2.3 Autenticación de la identidad individual

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

3.2.4 Información de abonado no verificada

Sin estipulación.

3.2.5 Validación de autoridad

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

3.2.6 Criterios de interoperación

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 de rutina

3.3.1.1 Renovación de certificados online

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

3.3.1.2. Renovación de certificados con personación

El proceso de identificación se efectuará del mismo modo que el de emisión de uno nuevo (apartado 4.3).

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

El proceso de identificación se efectuará del mismo modo que el de emisión de uno nuevo.

3.4 Identificación y autenticación para solicitud de revocación

Según lo expuesto 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

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

El proceso de solicitud difiere entre los certificados de Sede Electrónica, los certificados SSL OV, y los certificados SSL EV . Los detalles del proceso para cada uno de ellos son los siguientes:

4.1.1.1. Solicitud para certificados de Sede Electrónica

Se deberá presentar la referencia al Diario Oficial en el que aparece la disposición de creación de la Sede Electrónica. En dicha disposición deberá aparecer:

- Identificación del Diario Oficial, artículo y fecha de publicación
- Nombre de la Sede Electrónica
- URL de la Sede Electrónica
- Titular de la Sede Electrónica

La solicitud del certificado la deberá realizar un representante del Titular de la Sede Electrónica debidamente acreditado y autorizado para ello.

4.1.1.2. Solicitud para certificados OV

Para poder solicitar un Certificados de Servidor Web SSL OV la organización debe ser la poseedora del dominio.

El solicitante puede realizar la solicitud por los siguientes medios electrónicos:

- Por la Web de Firmaprofesional.
- Por correo electrónico.
- Enviando un formulario de solicitud facilitado por Firmaprofesional.

Firmaprofesional recibe la solicitud y comienza con el proceso de verificación.

4.1.1.3. Solicitud para certificados EV

Para la solicitud del certificado se seguirán los siguientes pasos:

1. Firma del contrato de suscriptor y la carta de autorización:

Un representante legal del solicitante debe firmar un contrato de suscriptor y una carta de autorización. El representante deberá tener poderes, al menos, para solicitar este tipo de certificados en nombre de su organización.

Además, firmará una carta de autorización, mediante la cual, autoriza a una persona o a varias a desempeñar el rol de aprobador de certificados. Mediante este rol, las personas autorizadas podrán solicitar y aprobar la emisión de los certificados. A partir de ese momento, se podrán solicitar certificados.

La firma de ambos documentos podrá realizarse de dos maneras.

- a. Manuscritamente. En este caso, el solicitante deberá enviar el contrato escaneado y firmado manuscritamente, por correo electrónico. Firmaprofesional verificará que el contrato lo ha firmado el representante realizando una llamada telefónica.
- b. Electrónicamente con un certificado cualificado de representante legal. En este caso, no sería necesaria ninguna verificación adicional.

2. Solicitud de los certificados:

La solicitud de certificados se realiza mediante un formulario PDF enviado desde el E-Mail de uno de los aprobadores de certificados. El hecho de solicitar la emisión supone también el hecho de aprobar la emisión del certificado, por parte de una de las personas relacionadas en el punto 1.3.3

En el proceso de solicitud de certificados SSL EV de Firmaprofesional se utilizarán, al menos, dos de las personas relacionadas en el punto 1.3.3.

4.1.1.4. Solicitud para certificados de PSD2

Para la solicitud del certificado se seguirán los siguientes pasos:

El Proveedor de Servicios de Pago presentará la solicitud del certificado junto con el certificado de ser proveedor de servicios de pago autorizado por la Autoridad competente, donde se incluirá el número de autorización, el rol del proveedor del servicio de pago y el nombre de la Autoridad Nacional Competente.

Los certificados de autenticación web cualificados de PSD2 se expiden solamente a personas jurídicas.

El solicitante puede realizar la firma de la documentación y la solicitud por los mismos medios que para los certificados EV descrito en el apartado "4.1.1.3. Solicitud para certificados EV", no siendo necesaria la carta de autorización".

4.1.2. Proceso de solicitud de certificados y responsabilidades

El solicitante deberá contactar con Firmaprofesional o con un Intermediario autorizado.

La gestión de las emisiones de este tipo de certificados únicamente podrá ser realizada por Firmaprofesional.

En los apartados 4.1.1.1, 4.1.1.2, 4.1.1.3 y 4.1.1.4, se describe el proceso concreto y documentación requerida para la solicitud de cada tipo de certificado.

4.2 Tramitación de las solicitudes de certificados

En el caso de los **certificados de Sede Electrónica**, el Operador de RA validará la veracidad y exactitud de los datos del solicitante y la sede electrónica, así como que el solicitante está en posesión de la clave privada asociada a la clave pública incluida en la petición de certificación. El Operador de RA generará la petición de certificado en un formato estándar y la enviará a Firmaprofesional.

Para tramitar los **certificados de SSL OV, SSL EV y PSD2**, el solicitante entregará a Firmaprofesional, directamente o a través de un intermediario autorizado, una petición de certificado en formato PKCS#10.

Firmaprofesional realizará la validación técnica de la petición PKCS#10 y la validación de los datos que contenga.

4.2.1 Realización de las funciones de identificación y autenticación

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

4.2.2 Aprobación o denegación de las solicitudes de certificados

Previa a la emisión del certificado de Sede Electrónica, 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 se cumplen los requisitos para que el certificado sea considerado que tiene un nivel de seguridad Alto conforme al documento de Perfiles de Certificados elaborado por el Gobierno de España, el certificado se emitirá con el OID correspondiente.

Previa a la emisión de los certificados SSL OV , SSL EV y PSD2, se valida la existencia de registro CAA para cada nombre DNS de las extensiones CN y subjectAltName del certificado. En el caso de que se emita el certificado, la validación se realizará antes del TTL

del registro CAA. Firmaprofesional procesa los tags "issue" e "issuewild". El registro CAA que identifica a dominios para los que se autoriza la emisión por parte de Firmaprofesional es "firmaprofesional.com".

Si la solicitud está firmada electrónicamente mediante un Certificado Corporativo de Representante Legal de Firmaprofesional o un certificado de Representante Legal de otra entidad que admita Firmaprofesional que haya garantizado el proceso de identificación conforme a la normativa española, ésta emitirá un Certificado de Servidor Web SSL EV; en otro caso, se emitirá un Certificado de Servidor Web SSL OV.

Adicionalmente, la emisión de Certificado de Servidor Web SSL EV requiere de la aprobación de dos personas: el Operador de la RA encargado de la gestión de la solicitud y Administrador del Departamento Técnico encargado de la emisión del certificado. El mismo requisito se exige para la emisión de un Certificado de PSD2

4.2.3 Tiempo de tramitación de las solicitudes de certificado

Según lo expuesto 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

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

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

Firmaprofesional hará entrega del certificado al solicitante permitiendo su descarga de forma segura desde Internet.

Los certificados de sede deben ser aceptados formalmente por el solicitante, dejando evidencia documental en poder de la RA.

4.4. Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

El proceso de aceptación de solicitud difiere entre los certificados de Sede Electrónica, de SSL OV, de SSL EV y de PSD2. Los detalles son los siguientes:

4.4.1.1 Aceptación de la solicitud para certificados de Sede Electrónica

Estos certificados únicamente son emitidos por la RA de Firmaprofesional.

El Operador de RA de Firmaprofesional verificará la disposición de creación de la Sede Electrónica así como la identidad de la persona solicitante y su capacidad de representación del Titular.

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.

4.4.1.1.1 Verificación del control del nombre de dominio

Para los certificados de Sede Electrónica Firmaprofesional sigue el mismo procedimiento de verificación del control del nombre de dominio que para los certificados EV. Para más información se puede consultar el apartado "3.2.2 Autenticación de la identidad de la organización e identidad de dominio" del presente documento.

4.4.1.2. Aceptación de la solicitud para certificados OV

El proceso de verificación se realiza cumpliendo con lo estipulado en la versión vigente del documento "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", emitido por CA/Browser Forum.

4.4.1.3. Aceptación de la solicitud para certificados EV

Los requisitos de verificación para la emisión de un Certificado de Servidor Web SSL EV de Firmaprofesional son los siguientes:

4.4.1.3.1. Verificación de la existencia legal e identidad del solicitante

Tipo de entidad	Aspectos a verificar	Métodos de verificación – Una de las siguientes opciones	Evidencia
Organización privada (Entidades no gubernamentales cuya creación fue gracias a un acto de incorporación a un registro legal)	<ul style="list-style-type: none"> - Existencia legal - Nombre de la organización - N° de registro o CIF - Registro oficial 	1) Consulta On-Line a: <ul style="list-style-type: none"> - Registro Mercantil. - Cámara de Comercio nacional. - O Legal Entity Identifier (LEI). 2) Certificado o documento expedido dos años antes de la emisión del certificado SSL por Registro Mercantil o equivalente, LEI o Cámara de Comercio.	Copia de la consulta o del certificado o documento expedido.
	Apoderamiento o Representación legal.	1) Consulta On-Line a: <ul style="list-style-type: none"> - Registro Mercantil. - Cámara de Comercio nacional. - O Legal Entity Identifier (LEI). 2) Documento Notarial. 3) Certificado o documento expedido dos años antes de la emisión del certificado SSL por Registro Mercantil o equivalente, LEI o Cámara de Comercio.	Copia de la consulta o del certificado o documento expedido.
Organización pública u organización gubernamental	<ul style="list-style-type: none"> - Existencia legal - Nombre de la organización - N° de registro o CIF 	1) Consulta a registro oficial. 2) Consulta LEI. 3) Certificado o documento expedido dos años antes de la emisión del certificado SSL por registro oficial o LEI.	Copia de la consulta o del certificado o documento expedido.
	- Apoderado o representante legal.	1) Bolefín oficial con nombramiento del cargo. 2) Documento oficial firmado por Fedatario Público o Poder notarial	Copia del documento.

Business Entity / Entidad Comercial (Cualquier entidad que no sea una organización privada, entidad pública o entidades no comerciales)	- Existencia legal - Nombre de la organización - N° de registro o CIF	1) Para Colegios profesionales: Estatutos de creación y su publicación en el BOE y tarjeta CIF, o LEI. 2) Para otros: Consulta a registro oficial público o LEI. 3) Certificado o documento expedido dos años antes de la emisión del certificado SSL por registro oficial o LEI.	Para Colegios: - Copia de los estatutos - Copia de la publicación en el BOE - Copia del CIF - O LEI - Copia del certificado o documento expedido. Para otros: - Copia de consulta. - O LEI. - Copia del certificado o documento expedido.
	- Apoderado o representante principal	Documento oficial de nombramiento, bien de la Junta general de la entidad, del registro público o poder notarial	Copia del documento oficial o poder notarial
Entidades no comerciales (Organización internacional)	- Existencia legal - Nombre de la organización - N° de registro o CIF	1) Documento de constitución. 2) LEI.	- Copia del documento de constitución - O LEI.
Marcas registradas o nombres comerciales (si una entidad desea que el certificado SSL EV incorpore su nombre comercial o una marca registrada). Su uso está limitado a los campos donde esa información pueda aparecer	- El solicitante ha registrado el nombre comercial o la marca registrada. - Vigencia del uso de la marca registrada o nombre comercial.	1) Consulta On-Line al registro oficial nacional. 2) Consulta On-Line al registro oficial internacional. 3) Certificado o documento expedido por el registro oficial nacional dos años antes de la emisión del certificado SSL.	Copia de la consulta o del certificado o documento expedido.

4.4.1.3.2. Verificación de la ubicación geográfica en la que el solicitante desarrolla su negocio

Tipo de entidad	Aspectos a verificar	Métodos de verificación – Una de las siguientes opciones	Evidencia
Para todos los tipos de organizaciones	- Ubicación geográfica en la que desarrolla su negocio el solicitante.	1) Si la ubicación geográfica del solicitante aparece en alguno de los métodos de verificación mencionados en el apartado de "Verificación de la existencia legal e identidad del solicitante", entonces no se realiza ninguna comprobación adicional. 2) Consulta a base de datos confiable. Por ejemplo, Legal Entity Identifier (LEI). 3) Documento notarial que certifique la ubicación geográfica.	Evidencias recogidas en el apartado "Verificación de la existencia legal e identidad del solicitante", copia de consulta a la base de datos confiable o copia del documento notarial.

4.4.1.3.3. Verificación de la existencia operativa del solicitante

Tipo de entidad	Aspectos a verificar	Métodos de verificación – Una de las siguientes opciones	Evidencia
Para todos los tipos de organizaciones	- Existencia operativa de la organización.	Todos los métodos descritos en los apartados "Verificación de la existencia legal e identidad del solicitante" y "Verificación de la ubicación geográfica en la que desarrolla su negocio el solicitante" verifican que la organización está en estado activo. Si no fuera posible, se realizaría una consulta On-Line a una base de datos confiable, como, Legal Entity Identifier (LEI).	Evidencias recogidas en el apartado "Verificación de la existencia legal e identidad del solicitante", copia de consulta a la base de datos confiable.

4.4.1.3.4. Verificación del control del nombre de dominio

Para los certificados EV Firmaprofesional sigue el mismo procedimiento de verificación del control del nombre de dominio que para los certificados OV. Para más información se

puede consultar el apartado “4.1.2.2.2. Verificación del control del nombre de dominio” del presente documento.

4.4.1.3.5. Verificación del nombre, cargo y autoridad del firmante del contrato de suscriptor y de aprobador del certificado

El solicitante deberá firmar un contrato de suscriptor y hacerle llegar al menos una copia escaneada a Firmaprofesional. En el contrato de suscriptor se establece que el solicitante podrá pedir a Firmaprofesional Certificados SSL EV para los dominios bajo su control y que tenga poder de utilizar.

El contrato deberá firmarlo la persona que actúe como firmante del contrato de suscriptor, según la definición de roles incluida en el punto 4.1.1.3.1 de esta Política.

El contrato incluye una declaración responsable, en la que reconoce que tiene autoridad y poderes para actuar en nombre del solicitante para pedir un certificado SSL EV a Firmaprofesional, hacer uso de él y custodiarlo. De este modo, se verifican los poderes del firmante del contrato de suscriptor.

El contrato del suscriptor irá acompañado de una carta de autorización, mediante la cual, el solicitante autoriza a personas concretas para desempeñar los roles descritos en el punto 4.1.1.3.1 de esta Política. De este modo, se verifican el nombre, el cargo, la oficina y la autoridad del aprobador de certificados.

4.4.1.3.6. Verificación de la firma del contrato de suscriptor.

Firmaprofesional utiliza uno de los siguientes métodos para verificar la firma del contrato de suscriptor:

1. Realizando una llamada telefónica al solicitante y haciendo un cuestionario de preguntas al firmante del contrato de suscriptor. La llamada es grabada y almacenada como evidencia.

2. Si el contrato de suscriptor es firmado con un certificado de representante legal de la organización solicitante, este se almacena como evidencia y no son necesarias más comprobaciones.

4.4.1.3.7. Verificación de la aprobación para la emisión de un certificado SSL EV.

Para poder emitir un certificado SSL EV, el aprobador de certificado autorizado mediante la carta de autorización (en la que aparece su dirección de correo electrónico) deberá enviar desde su correo electrónico la solicitud del certificado. Mediante este hecho ya estaría autorizando la emisión del certificado.

4.4.1.4. Aceptación de la solicitud para certificados de PSD2

Para verificar la información de la solicitud del certificado, Firmaprofesional validará dicha información comparándola contra el Registro Público de la Autoridad Nacional Competente (el registro público del Banco de España o el registro público de Autoridad Bancaria Europea-EBA, entre otros).

4.4.2 Publicación del certificado por la CA

Según lo expuesto 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

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

4.5 Uso de las claves y el certificado

4.5.1 Uso de la clave privada y del certificado por el suscriptor

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

4.5.2 Uso de la clave pública y del certificado por los terceros que confían en los certificados

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

4.6 Renovación del certificado sin cambio de claves

Sin estipulación.

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

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

4.7.1 Circunstancias para la renovación online con cambio de claves

Sin estipulación.

4.7.2 Quién puede pedir la renovación online de un certificado

Sin estipulación.

4.7.3 Tramitación de las peticiones de renovación online

Sin estipulación.

4.7.4 Notificación de la emisión del certificado renovado

Se siguen los mismos pasos que para la emisión de un nuevo certificado (apartado 4.3.2).

4.7.5 Forma de aceptación del certificado renovado

Se siguen los mismos pasos que para la emisión de un nuevo certificado.

4.7.6 Publicación del certificado renovado

Se siguen los mismos pasos que para la emisión de un nuevo certificado.

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

Se siguen los mismos pasos que para la emisión de un nuevo certificado.

4.8 Modificación de certificados

En caso de modificar algún dato, Firmaprofesional procederá a la revocación y a la emisión de un nuevo certificado.

4.8.1 Circunstancia de la modificación de 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

No está permitida la suspensión de ninguno de los tipos de certificados contemplados en esta política.

La revocación se realiza según se especifica en la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

4.9.1 Circunstancias para la revocación

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

4.9.2 Quién puede solicitar la revocación

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

4.9.3 Procedimientos de solicitud de revocación

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

4.9.4 Periodo de gracia de la solicitud de revocación

Sin estipulación.

4.9.5 Plazo en el que la CA debe resolver la solicitud de revocación

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

4.9.6 Obligación de verificación de las revocaciones por los terceros

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

4.9.7 Frecuencia de emisión de CRLs

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

4.9.8 Tiempo máximo entre la generación y la publicación de las CRLs

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

4.9.9 Disponibilidad del sistema en línea de verificación del estado de los certificados

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

4.9.10 Requisitos de comprobación de revocación en línea

Según lo expuesto 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 Necesidades especiales en relación con el compromiso de clave

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

4.9.13 Circunstancias para la suspensión

No está permitida la suspensión de ninguno de los tipos de certificados contemplados en esta política.

4.9.14 Quién puede solicitar la suspensión

Sin estipulación.

4.9.15 Procedimiento de solicitud de suspensión

No está permitida la suspensión de ninguno de los tipos de certificados contemplados en esta política.

4.9.16 Límites del periodo de suspensión.

Sin estipulación.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

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

4.10.2 Disponibilidad del servicio

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

4.10.3 Características adicionales

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

4.11 Finalización de la suscripción

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

4.12 Custodia y recuperación de claves

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

4.12.1 Política y prácticas fundamentales de custodia y recuperación

Sin estipulación.

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

Sin estipulación.

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

5.1 Controles físicos

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

5.1.1. Ubicación física y construcción

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

5.1.2. Acceso físico

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

5.1.3. Alimentación eléctrica y aire acondicionado

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

5.1.4 Exposición al agua

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

5.1.5. Protección y prevención de incendios

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

5.1.6. Sistema de almacenamiento

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

5.1.7 Eliminación de los soportes de información

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

5.1.8. Copias de seguridad fuera de las instalaciones

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

5.2 Controles de procedimiento

5.2.1. Roles de los responsables

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

5.2.2. Número de personas requeridas por tarea

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

5.2.3. Identificación y autenticación por rol

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

5.2.4. Roles que requieren segregación de funciones

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

5.3 Controles de personal

5.3.1. Requisitos relativos a la calificación, conocimiento y experiencia profesionales

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

5.3.2. Procedimientos de comprobación de antecedentes

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

5.3.3. Requerimientos de formación

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

5.3.4. Requerimientos y frecuencia de actualización de la formación

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

5.3.5. Frecuencia y secuencia de rotación de tareas

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

5.3.6. Sanciones por actuaciones no autorizadas

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

5.3.7. Requisitos de contratación de terceros

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

5.3.8. Documentación proporcionada al personal

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

5.4 Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

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

5.4.2. Frecuencia de procesado de registros de auditoría

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

5.4.3. Periodo de conservación de los registros de auditoría

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

5.4.4. Protección de los registros de auditoría

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

5.4.5. Procedimientos de respaldo de los registros de auditoría

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

5.4.6. Sistema de recogida de información de auditoría

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

5.5 Archivo de registros

5.5.1. Tipo de eventos archivos

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

5.5.2. Periodo de conservación de registros

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

5.5.3. Protección del archivo

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

5.5.4 Procedimientos de copia de seguridad del archivo

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

5.5.5 Requerimientos para el sellado de tiempo de los registros

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

5.5.6. Sistema de archivo de información de auditoría

Sin estipulación

5.5.7. Procedimientos para obtener y verificar información archivada

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

5.6 Cambio de claves de la CA

5.6.1. CA Raíz

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

5.6.2. CA Subordinada

Según lo expuesto 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 vulnerabilidades

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

5.7.2. Alteración de los recursos hardware, software y/o datos

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

5.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una Autoridad de Certificación o de la suite criptográfica

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

5.7.4. Continuidad de Negocio después de un desastre

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

5.8 Cese de actividad

5.8.1. Autoridad de Certificación

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

5.8.2. Autoridad de Registro

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

En concreto, en relación con la presente PC, las claves de firma serán generadas en los sistemas del solicitante utilizando sus propias aplicaciones compatibles con los estándares de PKI. Generalmente, las aplicaciones de servidores que pueden configurarse con el protocolo SSL, como IIS de Microsoft, incluye herramientas para generar claves y peticiones de certificados.

6.1.2 Entrega de la clave privada al firmante

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

6.1.3 Entrega de la clave pública al emisor del certificado

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

6.1.4 Entrega de la clave pública de la CA a los terceros que confían en los certificados

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

6.1.5. Tamaño de las claves

Deben ser claves RSA con una longitud mínima de 2.048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

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

6.1.7. Usos admitidos de la clave (campo KeyUsage de X.509v3)

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

6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos

6.2.1 Estándares para los módulos criptográficos

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

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

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

6.2.3 Custodia de la clave privada

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

6.2.4. Copia de seguridad de la clave privada

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

6.2.5. Archivo de la clave Privada

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

6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico

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

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

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

6.2.8. Método de activación de la clave privada

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

6.2.9. Método de desactivación de la clave privada

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

6.2.10 Método de destrucción de la clave privada

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

6.2.11 Clasificación de los módulos criptográficos

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

6.3. Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

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

6.3.2 Periodos de operativos de los certificados y periodo de uso para el par de claves

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

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

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

6.4.2 Protección de los datos de activación

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

6.4.3 Otros aspectos de los datos de activación

Sin estipulación

6.5 Controles de seguridad informática

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

6.5.1 Requerimientos técnicos de seguridad específicos

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

6.5.2. Evaluación de la seguridad informática

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

6.6. Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

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

6.6.2 Controles de gestión d seguridad

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

6.6.3 Gestión del ciclo de vida del hardware criptográfico

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

6.7 Controles de seguridad en la red

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

6.8. Fuente de tiempo

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

7. Perfiles de los certificados, CRL y OCSP

7.1 Perfil de los certificados

En la Declaración de Prácticas de Firmaprofesional se describe el perfil común a todos los certificados.

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
Sede Electrónica Nivel Alto	1.3.6.1.4.1.13177.10.1.20.1
Sede Electrónica Nivel Medio	1.3.6.1.4.1.13177.10.1.20.2
SSL OV	1.3.6.1.4.1.13177.10.1.3.1
SSL EV / Cualificado y PSD2	1.3.6.1.4.1.13177.10.1.3.10

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>).

7.1.1 Número de versión

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

7.1.2. Extensiones de los certificados

En el documento "Perfiles de Certificados de Firmaprofesional" se especificará las extensiones requeridas para cada tipo de certificado contemplados en la presente política.

7.1.3. Identificadores de objeto (OID) de los algoritmos utilizados

De acuerdo con el apartado 7.1 de la presente política.

7.1.4. Formatos de nombres

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

7.1.5. Restricciones de los nombres

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

7.1.6. Identificador de objeto (OID) de la Política

Los OID de cada certificado incluido en la presente política se encuentra detallado en los apartados 1.2 y 7.1 de la presente política.

7.1.7 Extensión del uso de las restricciones de política

Sin estipulación.

7.1.8 Sintaxis y semántica de los “PolicyQualifier”

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

7.1.9 Tratamiento semántico para la extensión “Certificate Policy”

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

7.2 Perfil de CRL

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

7.2.1 Número de versión

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

7.2.2 CRL y extensiones

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

7.3 Perfil de OCSP

7.3.1 Número de versión

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

7.3.2 OCSP y extensiones

Sin estipulación.

8. Auditorías de cumplimiento y otros controles

8.1. Frecuencia de las auditorías

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

8.2. Cualificación del auditor

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

8.3 Relación entre el auditor y la autoridad auditada

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

8.4 Aspectos cubiertos por los controles

8.4.1 Auditorías en las Autoridades de Registro

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

8.5 Acciones a emprender como resultado de la detección de incidencias

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

8.6 Comunicación de resultados

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

9. Otras cuestiones legales y de actividad

9.1 Tarifas

Firmaprofesional podrá establecer las tarifas que considere oportunas a los suscriptores, así como establecer los medios de pago que considere más adecuados 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 de certificado o renovación

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

9.1.2 Tarifas de acceso a los certificados

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

9.1.3 Tarifas de acceso a la información de estado o revocación

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

9.1.4 Tarifas de otros servicios

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

9.1.5 Política de reembolso

Sin estipulación.

9.2 Responsabilidades económicas

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

9.2.1 Cobertura de seguro

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

9.2.2 Otros activos

Sin estipulación.

9.2.3 Seguro o cobertura de garantía para las entidades finales

Sin estipulación.

9.3 Confidencialidad de la información

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

9.3.1 Ámbito de la información confidencial

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

9.3.2 Información no confidencial

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

9.3.3 Responsabilidad en la protección de información confidencial

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

9.4.2 Información tratada como privada

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

9.4.3 Información no calificada como privada

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

9.4.4. Responsabilidad de la protección de los datos de carácter personal

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

9.4.5 Comunicación y consentimiento para usar datos de carácter personal

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

9.4.6 Revelación en el marco de un proceso judicial

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

9.4.7 Otras circunstancias de publicación de información

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

9.5 Derechos de propiedad intelectual

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

9.6 Obligaciones

9.6.1 Obligaciones de la CA

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

9.6.2 Obligaciones de la RA

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

9.6.3 Obligaciones de los solicitantes

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

9.6.4 Obligaciones de los terceros que confían en los certificados

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

9.6.5 Obligaciones de otros participantes

Sin estipulación.

9.7 Exención de garantía

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

9.8 Responsabilidades

9.8.1 Responsabilidades de la Autoridad de Certificación

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

9.8.2 Responsabilidades de la Autoridad de Registro

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

9.8.3 Responsabilidades del suscriptor

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

9.8.4 Delimitación de responsabilidades

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

9.9 Indemnizaciones

9.9.1 Alcance de la cobertura

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

9.9.2 Cobertura de seguro y otras garantías para los terceros aceptantes

No existe cobertura para los terceros aceptantes.

9.9.3 Limitaciones de pérdidas

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

9.10 Periodo de validez

9.10.1 Plazo

La presente CP entrará en vigor en el momento de su publicación.

9.10.2 Sustitución y derogación de la CPS

La presente CP, será derogada en el momento que una nueva versión del documento sea publicada.

La nueva versión sustituirá íntegramente el documento anterior.

9.10.3 Efectos de la finalización

Para los certificados vigentes emitidos bajo una CP anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11 Notificaciones individuales y comunicación con los participantes

De modo general, se utilizará el sitio web de Firmaprofesional www.firmaprofesional.com para realizar cualquier tipo de notificación y comunicación.

Si el suscriptor de certificados de autenticación de sitios Web detecta cualquier problema con el certificado podrá notificarlo por e-mail a soporte@firmaprofesional.com

Cualquier correo que se envía a esta dirección de correo entra en el Sistema de Atención al Cliente de Firmaprofesional.

En caso de que se produzcan modificaciones sobre información relevante sobre PSD2 del proveedor del servicio de pago que pueda afectar a la validez del certificado, el Banco de España o Autoridad Nacional Competente lo comunicará a través de la cuenta soporte@firmaprofesional.com.

9.12 Cambios en las especificaciones

9.12.1 Procedimiento para los cambios

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

9.12.2 Periodo y procedimiento de notificación

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

9.12.3 Circunstancias en las que el OID debe ser cambiado

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

9.13 Reclamaciones y resolución de conflictos

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

9.14 Normativa aplicable

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

9.15 Cumplimiento de la normativa aplicable

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

9.16 Estipulaciones diversas

9.16.1 Cláusula de aceptación completa

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

9.16.2 Independencia

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

9.16.3 Resolución por la vía judicial

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

9.17 Otras provisiones

Sin estipulación.