firmaprofesional

Política de Servicio Cualificado

Declaración de Prácticas y Política de Servicio (SPPS) de Firma Electrónica Cualificada Remota de Firmaprofesional, S.A.

Versión: 230413

Clasificación: Confidencial

BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL 3B6
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

FIRMAPROFESIONAL, S.A.
2023.04.14 12:58:50 +02'00'

Restricciones de utilización y revelación de los datos contenidos en este documento.

© Abril 2023 Firmaprofesional, S.A.

Este documento es confidencial y propiedad de Firmaprofesional, y no puede ser empleado para ningún propósito diferente a la presentación de esta propuesta.

En ningún caso el documento o cualquiera de sus partes podrán ser distribuidas a terceros sin el consentimiento explícito y por escrito de Firmaprofesional.

Asimismo, ninguna de las partes del documento puede ser copiada, fotografiada, fotocopiada, transmitida electrónicamente, almacenada en un sistema de gestión documental, o reproducida mediante cualquier sistema, sin autorización previa y por escrito de Firmaprofesional.

Histórico de versiones

Versión	Sección y cambios	Fecha
220308	• Versión inicial	08/03/2022
230216	• Revisión anual	16/02/2023
230413	• Actualización apartado 4.3.1	13/04/2023

Índice

1. Introducción **10**
1.1. Resumen 10
1.2. Identificación del documento 10
1.3. Entidades Participantes 11
1.3.1 Autoridades de Certificación (CA) 11
1.3.2 Autoridad de Registro (RA) 11
1.3.3 Suscriptores 12
1.3.3.1 Solicitante 12
1.3.3.2 Firmante 14
1.3.4 Terceros que confían en los certificados 14
1.3.5 Otros participantes 14
1.4 Uso de los certificados 15
1.4.1 Usos apropiados de los certificados 15
1.4.1.1 Periodo de validez de los certificados 15
1.4.1.2 Dispositivos Cualificados de Creación de Firma 15
1.4.2 Usos prohibidos de los certificados 16
1.5 Administración de Políticas 16
1.5.1 Organización que administra el documento 16
1.5.2 Persona de contacto 16
1.5.3 Persona que determina la idoneidad de la CP para la póliza 17
1.5.4 Procedimiento de aprobación de la CP 17
1.6 Definiciones y siglas 17
2. Repositorios y publicación de información **17**
2.1 Repositorios 17
2.2 Publicación de información de certificación 17
2.3 Hora o frecuencia de publicación 17
2.4 Control de acceso a los repositorios 17
3. Identificación y autenticación 18
3.1 Registro de Nombres 18
3.1.1 Tipos de nombres 18
3.1.2 Necesidad de que los nombres sean significativos 18
3.1.3 Anonimato o seudónimo de los suscriptores 18
3.1.4 Reglas para interpretar varias formas de nombres 18
3.1.5 Unicidad de los nombres 18
3.1.6 Reconocimiento, autenticación y función de las marcas 19
3.2 Validación inicial de la identidad 19
3.2.1 Método de prueba de posesión de clave privada 19
3.2.2 Autenticación de la identidad de la organización e identidad de dominio 19
3.2.3 Autenticación de la identidad de una persona física 19
3.2.4 Información de suscriptor no verificada 19

3.2.5 Validación de la identidad de la RA y de operadores de la RA 19
3.2.6 Criterios de interoperabilidad 19
3.3 Identificación y autenticación para solicitudes de renovación de claves 20
3.3.1 Identificación y autenticación para el cambio de clave 20
3.3.2 Identificación y autenticación para la renovación de certificados tras su revocación 20
3.4 Identificación y autenticación para solicitud de revocación 20
4. Requisitos operacionales del ciclo de vida de las claves de firma 20
4.1. Solicitud de certificados 20
4.1.1 Quién puede enviar una solicitud de certificado 20
4.1.2 Proceso de solicitud de certificados y responsabilidades 21
4.2. Tramitación de las solicitudes de certificados 21
4.2.1 Realización de las funciones de identificación y autenticación 21
4.2.2 Aprobación o denegación de las solicitudes de certificados 21
4.2.3 Tiempo de tramitación de las solicitudes de certificado 22
4.3. Emisión de certificados e Inicialización de las claves de firma 22
4.3.1 Acciones de la CA durante la emisión del certificado 22
4.3.1.1. Generación de las claves de firma 22
4.3.1.2. Asociación de los medios de identificación electrónica del firmante 23
4.3.1.3. Asociación del certificado del firmante 24
4.3.1.4. Provisión de los medios de identificación del firmante 24
4.3.2 Notificación al suscriptor por parte de la CA de la emisión del certificado y entrega 24
4.4. Aceptación 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 las claves y el certificado 25
4.5.1. Uso de certificado y clave privada del suscriptor 25
4.5.1.1. Activación de las claves de firma 25
4.5.1.2. Gestión de los datos de activación de firma 27
4.5.1.3. Borrado de las claves de firma 27
4.5.1.4. Copia de seguridad y restauración de la claves de firma 28
4.5.2 Uso de certificados y claves públicas de parte que confía 28
4.6 Renovación del certificado (sin cambio de claves) 28
4.6.1 Circunstancia para la renovación del certificado 28
4.6.2 Quién puede solicitar la renovación 29
4.6.3 Procesamiento de solicitudes de renovación de certificados 29
4.6.4 Notificación al suscriptor de la emisión de un nuevo certificado 29
4.6.5 Conducta que constituye la aceptación de un certificado de renovación 29
4.6.6 Publicación del certificado de renovación por parte de la CA 29
4.6.7 Notificación de la emisión del certificado por parte de la CA a otras entidades 29
4.7 Renovación del certificado con cambio de clave 30
4.7.1 Circunstancia para el cambio de clave del certificado 30
4.7.2 Quién puede solicitar la certificación de una nueva clave pública 30

4.7.3 Procesamiento de solicitudes de cambio de claves de certificados 30
4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado 30
4.7.5 Conducta que constituye la aceptación de un certificado con clave nueva 30
4.7.6 Publicación del certificado con nueva clave por parte de la CA 31
4.8 Modificación del certificado 31
4.8.1 Circunstancia para la modificación del certificado 31
4.8.2 Quién puede solicitar la modificación del certificado 31
4.8.3 Procesamiento de solicitudes de modificación de certificados 31
4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado 31
4.8.5 Conducta que constituye la aceptación del certificado modificado 31
4.8.6 Publicación del certificado modificado por la CA 31
4.8.7 Notificación de la emisión del certificado por parte de la CA a otras entidades 32
4.9 Revocación y suspensión de certificados 32
4.9.1 Circunstancias para la revocación 32
4.9.2 Quién puede solicitar la revocación 32
4.9.3 Procedimiento de solicitud de revocación 32
4.9.4 Periodo de gracia de la solicitud de revocación 32
4.9.5 Tiempo dentro del cual CA debe procesar la solicitud de revocación 32
4.9.6 Requisito de verificación de revocación para las partes que confían 33
4.9.7 Frecuencia de emisión de CRL 33
4.9.8 Latencia máxima para las CRL 33
4.9.9 Disponibilidad de verificación de estado / revocación en línea 33
4.9.10 Requisitos de verificación de revocación en línea 33
4.9.11 Otras formas de anuncios de revocación disponibles 33
4.9.12 Requisitos especiales relacionados con el compromiso clave 33
4.9.13 Circunstancias para la suspensión 34
4.9.14 Quién puede solicitar la suspensión 34
4.9.15 Procedimiento de solicitud de suspensión 34
4.9.16 Límites del período de suspensión 34
4.10 Servicios de estado de certificados 34
4.10.1 Características operativas 34
4.10.2 Disponibilidad del servicio 34
4.10.3 Funciones opcionales 35
4.11 Finalización de la suscripción 35
4.12 Custodia y recuperación de claves 35
4.12.1 Política y prácticas de custodia y recuperación de claves 35
4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión 35
5. Controles de seguridad física, de gestión y de operaciones 36
5.1. Controles de seguridad física 36
5.1.1 Ubicación y construcción del sitio 36
5.1.2 Acceso físico 36
5.1.3 Energía y aire acondicionado 36
5.1.4 Exposición al agua 36
5.1.5 Prevención y protección contra incendios 36

5.1.6 Almacenamiento de medios 36
5.1.7 Eliminación de residuos 37
5.1.8 Respaldo fuera de las instalaciones 37
5.2. Controles de procedimientos 37
5.2.1 Roles de confianza 37
5.2.2 Número de personas necesarias por tarea 38
5.2.3 Identificación y autentificación para cada rol 38
5.2.4 Roles que requieren separación de funciones 38
5.3. Controles de personal 38
5.4. Procedimientos de auditoría de seguridad 39
5.5. Archivo de informaciones 40
5.6. Cambio de claves 40
5.7. Compromiso de claves y recuperación de desastre 40
5.8 Cese de actividad 40
6 Controles de seguridad técnica 41
6.1. Operaciones y sistemas 41
6.2. Protección de la clave privada y controles de ingeniería de los módulos criptográficos 41
6.3. Otros aspectos de la gestión del par de claves 41
6.4. Datos de activación 41
6.5. Controles de seguridad informática 41
6.6. Controles técnicos del ciclo de vida 42
6.7.Controles de seguridad de red 42
6.8 Control de tiempo 42
7. Perfiles de los certificados, CRL y OCSP 43
7.1 Perfil del certificado 43
7.1.1 Número(s) de versión 43
7.1.2 Extensiones del certificado 43
7.1.3 Identificadores de objetos de algoritmos 43
7.1.4 Formas del nombre 43
7.1.5 Restricciones del nombre 43
7.1.6 Identificador del objeto de la política del certificado 43
7.1.7 Uso de la extensión Policy Constraints 44
7.1.8 Sintaxis y semántica de los calificadores de política 44
7.1.9 Semántica de procesamiento de la extensión critical Certificate Policies 44
7.2 Perfil CRL 45
7.2.1 Número(s) de versión 45
7.2.2 Extensiones de CRL y entradas de CRL 45
7.3 Perfil OCSP 45
7.3.1 Número(s) de versión 45
7.3.2 Extensiones OCSP 45
8. Auditorías de cumplimiento y otros controles 46
8.1 Frecuencia de las auditorías 46
8.2 Cualificación del auditor o evaluador 46
8.3 Relación entre el auditor y la autoridad auditada 46

8.4 Aspectos cubiertos por la evaluación 46
8.5 Acciones a emprender como resultado de la detección de deficiencias 46
9. Otras cuestiones legales y de actividad 47
9.1 Tarifas 47
9.1.1 Tarifas de emisión o renovación de certificados 47
9.1.2 Tarifas de acceso a los certificados 47
9.1.3 Tarifas de acceso a la información de revocación o de estado 47
9.1.4 Tarifas por otros servicios 47
9.1.5 Tarifas de reembolso 48
9.2 Responsabilidades económicas 48
9.2.1 Cobertura del seguro 48
9.2.2 Otros activos 48
9.2.3 Cobertura de seguro o garantía para las entidades finales 48
9.3 Confidencialidad de la información comercial 48
9.3.1 Alcance de la información confidencial 48
9.3.2 Información no confidencial 48
9.3.3 Responsabilidad de proteger la información confidencial 49
9.4 Protección de la información personal 49
9.4.1 Política de protección de datos de carácter personal 49
9.4.2 Información tratada como privada 49
9.4.3 Información no considerada privada 49
9.4.4 Responsabilidad de proteger la información privada 49
9.4.5 Aviso y consentimiento para el uso de la información privada 49
9.4.6 Divulgación en virtud de un proceso judicial o administrativo 50
9.4.7 Otras circunstancias de divulgación de información 50
9.5 Derechos de propiedad intelectual 50
9.6 Obligaciones y garantías 50
9.6.1 Obligaciones de la AC 50
9.6.2 Obligaciones de la AR 50
9.6.3 Obligaciones de los solicitantes 50
9.6.4 Representaciones y garantías de los terceros que confían en los certificados 51
9.6.5 Declaraciones y garantías de otros participantes 51
9.7 Exención de garantía 51
9.8 Limitaciones de responsabilidad 51
9.9 Indemnizaciones 51
9.10 Periodo de validez y terminación 52
9.10.1 Plazo 52
9.10.2 Terminación 52
9.10.3 Efecto de la terminación y supervivencia 52
9.11 Avisos y comunicaciones individuales con los participantes 52
9.12 Modificaciones o cambios en las especificaciones 52
9.12.1 Procedimiento para los cambios 52
9.12.2 Mecanismo y plazo de notificación 52
9.12.3 Circunstancias en las que debe modificarse la OID 53

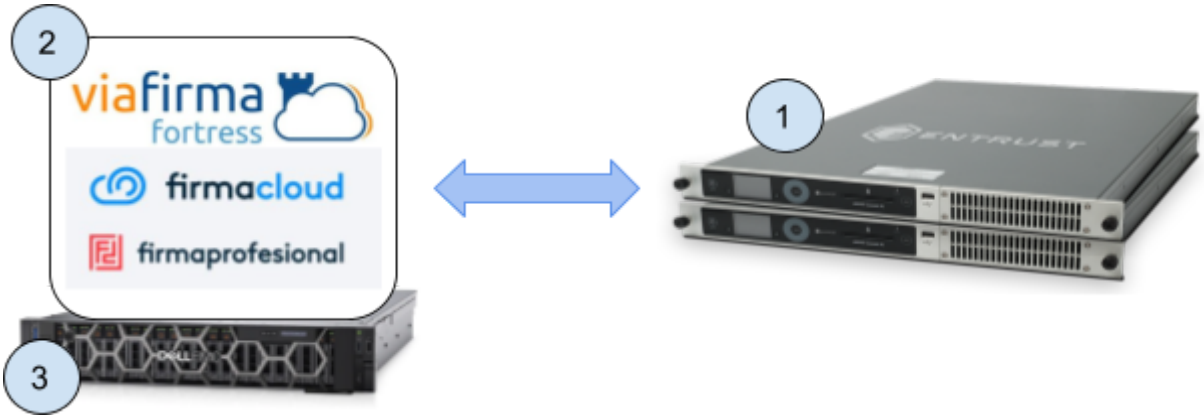
9.13 Disposiciones para la resolución de conflictos 53
9.14 Normativa aplicable 53
9.15 Cumplimiento de la normativa aplicable 53
9.16 Disposiciones diversas 53
9.16.1 Acuerdo completo 53
9.16.2 Independencia 53
9.16.3 Resolución por vía judicial 54
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos) 54
9.16.5 Fuerza mayor 54
9.17 Otras disposiciones 54

1. Introducción

1.1. Resumen

El sistemas de generación de firmas electrónicas cualificados remotas de Firmaprofesional está formado por los siguientes elementos:

1. HSM nCipher Connect 1.500 y Connect 6.000
2. Software Viafirma Fortress *hardenizado* en colaboración con Firmaprofesional
3. Servidor DELL EMC *tamper proof* modelo Power Edge R440, Intel Xeon Silver 4210R 2.4G, 2x 16GB RAM RDIMM, 2x 480GB SSD SATA



1.2. Identificación del documento

Nombre:	Declaración de Prácticas y Política de Servicio de Firma electrónica cualificada remota de Firmaprofesional, S.A.
Versión:	230413
Descripción:	Declaración de Prácticas y Política de Servicio de Firma electrónica cualificada remota de Firmaprofesional, S.A.
Fecha de Emisión:	13/04/2023
OID	1.3.6.1.4.1.13177.30.8.1
Localización	http://www.firmaprofesional.com/cps

1.3. Entidades Participantes

1.3.1 Autoridades de Certificación (CA)

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

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

1.3.2 Autoridad de Registro (RA)

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

Cada Autoridad de Registro establecerá:

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

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

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

1.3.3 Suscriptores

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

Dependiendo del tipo de Certificado, el Suscriptor puede ser:

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

1.3.3.1 Solicitante

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

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

- Los Certificados Corporativos de Colegiado:
    - Cualquier profesional colegiado en un colegio profesional.
    - El propio Colegio Profesional, en nombre y asistencia del colegiado.

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

1.3.3.2 Firmante

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

1.3.4 Terceros que confían en los certificados

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

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

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

1.3.5 Otros participantes

Sin estipulación.

1.4 Uso de los certificados

1.4.1 Usos apropiados de los certificados

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

Asimismo, los certificados emitidos bajo este documento pueden ser utilizados con los siguientes propósitos:

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

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

1.4.1.1 Periodo de validez de los certificados

Según la Política de Certificación correspondiente del certificado emitido.

1.4.1.2 Dispositivos Cualificados de Creación de Firma

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

- Extensión "Certificate Policies" con valor OID de la política de certificación propia de Firmaprofesional correspondiente al certificado de Nivel Alto con DCCF portable o centralizado

- Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" habilitado.

1.4.2 Usos prohibidos de los certificados

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta CP y en la CPS.

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

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

1.5 Administración de Políticas

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

1.5.1 Organización que administra el documento

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

1.5.2 Persona de contacto

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

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

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

1.5.4 Procedimiento de aprobación de la CP

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

1.6 Definiciones y siglas

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

2. Repositorios y publicación de 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.

3.1.1 Tipos de nombres

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

3.1.2 Necesidad de que los nombres sean significativos

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

3.1.3 Anonimato o seudónimo de los suscriptores

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

3.1.4 Reglas para interpretar varias formas de nombres

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

3.1.5 Unicidad de los nombres

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

3.1.6 Reconocimiento, autenticación y función de las marcas

Sin estipulación

3.2 Validación inicial de la identidad

3.2.1 Método de prueba de posesión de clave privada

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

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

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

3.2.3 Autenticación de la identidad de una persona física

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

3.2.4 Información de suscriptor no verificada

Sin estipulación.

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

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

3.2.6 Criterios de interoperabilidad

En la actualidad Firmaprofesional no dispone de certificación cruzada.

3.3 Identificación y autenticación para solicitudes de renovación de claves

3.3.1 Identificación y autenticación para el cambio de clave

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

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

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

3.4 Identificación y autenticación para solicitud de revocación

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

4. Requisitos operacionales del ciclo de vida de las claves de firma

4.1. Solicitud de certificados

4.1.1 Quién puede enviar una solicitud de certificado

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

4.1.2 Proceso de solicitud de certificados y responsabilidades

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

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

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

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

4.2. Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

4.2.2 Aprobación o denegación de las solicitudes de certificados

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

4.2.3 Tiempo de tramitación de las solicitudes de certificado

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

4.3. Emisión de certificados e Inicialización de las claves de firma

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

4.3.1 Acciones de la CA durante la emisión del certificado

4.3.1.1. Generación de las claves de firma

El SSASC utiliza la aplicación de firma en servidor "firmacloud" en combinación con un módulo criptográfico (HSM) que actúa como SCDev / QSCD, el cual es un dispositivo cualificado de creación de firma.

El SSASC utiliza HSMs ha sido validado para cumplir con al menos FIPS 140-2 nivel 3, FIPS 140-3 nivel 3, o un perfil de protección de criterios comunes apropiado o un objetivo de seguridad, EAL 4 (o superior) para realizar todas las operaciones criptográficas con las claves de los firmantes **[SRG_KM.1.1]**

Las claves de los firmantes son claves RSA con una longitud de clave de 2048 bits. **[SRG_KM.1.2]**

Fuera del módulo HSM las claves se almacenan cifradas con el algoritmo AES y una longitud de clave de 128 bits. La clave de cifrado es única y se deriva de una clave maestra del módulo HSM. **[SRG_KM.1.3]**

Las operaciones de inicialización de la administración del módulo criptográfico requieren de control dual. **[SRG_KM.1.4]**

Los pares de claves de los firmantes son generados en la primera fase del proceso de emisión del certificado electrónico del firmante.

Antes de importar el certificado del firmante, el par de claves del firmante se encuentra en estado no activo y el SSASC no permite su uso. **[SRC_SKS.1.3]**

Junto a la clave del firmante el SSASC genera una petición de certificado en formato PKCS#10 que sirve como prueba de posesión de la clave privada del firmante en el proceso de registro del certificado y emisión del certificado por parte de la Autoridad de Certificación.

4.3.1.2. Asociación de los medios de identificación electrónica del firmante

El operador de la Autoridad de Registro se autentica mediante certificado cliente por canal seguro a la interfaz de la Autoridad de Registro.

La Autoridad de Registro valida la identidad del firmante de acuerdo con los requisitos establecidos en la Declaración de Prácticas de Certificación del certificado solicitado por el firmante con un nivel de garantía alto según los requisitos establecidos en UE 2015/1502. **[LNK-6.2.2-01] [LNK-6.2.2-02]**

No se delegan partes del proceso de identificación y autenticación del firmante para el acto de firma a terceras partes.

La Autoridad de registro almacena los datos del firmante, entre ellos, su número de teléfono y solicita al SSASC la creación de un par de claves que vincula en la base de datos al firmante. **[LNK-6.2.2-03]**

La Autoridad de Registro solicita a la Autoridad de Certificación el certificado electrónico vinculado al par de claves generado en el SSASC.

La Autoridad de Registro pide al SSASC que vincule el certificado emitido al par de claves del firmante. **[LNK-6.2.2-05]**

La Autoridad de Registro entregará mediante correo electrónico al firmante un código único de registro de un solo uso para completar el proceso de alta.

Los medios de identificación electrónica del firmante son generados por el firmante accediendo con un navegador web mediante protocolo seguro al SSASC.

Una vez el SSASC comprueba que el usuario ha activado dos factores de autenticación de diferentes categorías activa el uso de la clave privada del firmante.

El SSA protege la integridad de las claves de los firmantes y sus metadatos asociados mediante la asociación en base de datos **[LNK-6.2.2-10]**

4.3.1.3. Asociación del certificado del firmante

Una vez el proceso de registro y emisión del certificado del firmante se ha completado, el certificado del firmante es importado en el SSASC.

El SSASC verifica que la clave pública en el certificado del firmante y la almacenada en el sistema se corresponden **[LNK-6.2.3-01]**.

En caso de que ambas claves públicas coincidan, el certificado queda vinculado al par de claves del firmante.

La clave del firmante es marcada como inactiva y queda a la espera de que el firmante active sus factores de activación de firma. [**LNK-6.2.3-02]**.

El SSASC protege la integridad de las claves de los firmantes y sus metadatos asociados mediante la asociación en base de datos. **[LNK-6.2.3-03] [SRC_SKS.1.5]**

4.3.1.4. Provisión de los medios de identificación del firmante

Los medios de identificación del firmante son generados por el propio firmante, accediendo con un navegador web mediante protocolo seguro al SSASC.

La semilla de las contraseñas de uno solo uso (OTP) reside cifrada en la base de datos del SSASC y protegida por una clave AES protegida a su vez por el módulo criptográfico y es generada de forma aleatoria por el SAM.

El SSASC en ningún caso almacena las contraseñas del firmante, solo hashes para poder comprobar su validez.

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

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

4.4. Aceptación del certificado

4.4.1 Forma en la que se acepta el certificado

El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el suscriptor y Firmaprofesional haya sido firmado y el certificado haya sido entregado, ya sea personal o telemáticamente.

Como evidencia de la aceptación deberá quedar una hoja de aceptación firmada por el firmante. El certificado se considerará válido a partir de la fecha en que se firmó la hoja de aceptación.

Si la hoja de aceptación es en formato electrónico, el firmante podrá firmarla por medio de una firma electrónica.

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 las claves y el certificado

4.5.1. Uso de certificado y clave privada del suscriptor

4.5.1.1. Activación de las claves de firma

Para cada uso de su clave de firma, el firmante ha de proveer un mensaje de activación de firma (SAD) mediante el protocolo de activación de firma (SAP). El mensaje ha de contener dos factores de autenticación de diferente tipo y un testigo de sesión. **[SIG-6.3.1-01] [SIG-6.3.1-05]**

Para obtener un testigo de sesión, el SSASC requiere que el firmante se identifique previamente con su usuario y al menos un factor de autenticación.

Las claves del firmante solo se pueden activar si el módulo HSM se encuentra activo. **[SIG-A.5-02]**

La clave de un firmante solo es activable si el firmante completa el protocolo de activación (SAP) y los factores de autenticación enviados en el SAD son correctos. **[SIG-6.3.1-09]**

El protocolo de activación de firma (SAP) está diseñado para prevenir ataques de man-in-the-middle y replay **[SIG-6.3.1-02]**. Además de esto el mensaje SAD incorpora protecciones contra suplantación, robo de sesión, duplicación, robo de credenciales, phishing escucha y adivinación, mediante la combinación de técnicas de cifrado, firma electrónica, funciones resumen, incorporación de datos aleatorios y de dos factores de autenticación de diferente naturaleza (algo que el firmante conoce y algo que firmante posee). Si el firmante introduce erróneamente 3 veces consecutivas el factor de activación el acceso a la clave remota queda bloqueado. Una clave remota bloqueada solo puede ser desbloqueada por el propio firmante mediante la introducción de recuperación enviado a su correo electrónico **[SIG-6.3.1-06] [SIG-A.5-04] [SIG-A.5-06] [SIG-A.5-07]**

Los factores de activación se transportan siempre a través de un protocolo de comunicación seguro dentro del mensaje de activación de clave (SAD) **[SIG-A.5-03]**

Los controles de acceso implementados en el SSASC garantizan que un firmante no tiene acceso las claves de otros firmantes ni a otros objetos y funciones del sistema que no sean las funciones de firma o su gestión personal **[SIG-6.3.1-03]**

El mensaje de activación de firma (SAD) vincula el resumen criptográfico de los datos a firmar con los datos de activación del firmante mediante el testigo de sesión incluido en el mensaje. **[SIG-6.3.1-04]**

Una vez se activa la clave del firmante el SSASC solo permite su uso para firmar el resumen criptográfico contenido en el mensaje SAD utilizado para la activación **[SIG-6.3.1-07]**. Una vez se realiza la operación de firma solicitada con el SAD el SSASC desactiva la clave del firmante, requiriendo de un nuevo SAD para una nueva firma.

El SSA almacena en los metadatos del par de claves del firmante la fecha de caducidad del certificado asociado. Antes del uso de una clave de firma el SSASC comprueba que la fecha de caducidad del certificado es válida y el estado de revocación del certificado, y deniega la operación acorde al estado del certificado. **[SIG-6.3.1-08]**

Todas las comunicaciones con el SSASC están protegidas mediante el protocolo TLS 1.2.

El SSASC permite generar firmas RSA PKCS#1 v1.5 y algoritmo de resumen SHA-256. **[SIG-6.3.1-10]**

4.5.1.2. Gestión de los datos de activación de firma

El mensaje con los datos de activación de firma (SAD) es generado a partir de un código de un solo uso generado en una aplicación a partir de un semilla previa o recibido vía SMS generado por el mismo SSASC **[SIG-A.6-02]**

El mensaje del SAD contiene el resumen(es) criptográfico(s) de los datos a firmar, referencias que permiten identificar la clave seleccionada e identificar al firmante, el PIN de activación de firma cifrado. Todo el mensaje del SAD se firma con la clave privada de activación de firma en la aplicación SAA para autenticar al firmante. **[SIG-A.6-01] [SIG-A.6-03] [SIG-A.6-06]**

El SSASC solo permite que el firmante pueda utilizar su clave de activación de firma desde un único teléfono inteligente evitando así su duplicado. **[SIG-A.6-06]**

La combinación de dos factores de autenticación de diferente naturaleza y el token de sesión, aseguran que el firmante tiene control exclusivo de sus datos de activación de firma. **[SIG-A.6-07]**

El SAP consiste en la transmisión de un solo mensaje SAD a través de un canal seguro hasta el SSA. El módulo de activación de firma (SAM) es un sub-módulo del SSA **[SIG-A.6-05]**

El nivel AVA_VAN.5 de evaluación de la solución SSA ha considerado atacantes de potencial alto en las pruebas de seguridad con el fin de asegurar que el mecanismo de autenticación para activar los datos de creación de firma no puede ser alterado. **[SIG-A.6-08]**

4.5.1.3. Borrado de las claves de firma

Las claves del firmante son borradas de forma inmediata, cuando el certificado del firmante es revocado.

Periódicamente Firmaprofesional ejecuta un proceso de borrado de aquellas claves de los firmantes cuyo certificado asociado ha caducado. **[DEL-6.3.2-01]**

Los firmantes podrán solicitar la revocación de su certificado electrónico siguiendo los mecanismos establecidos en la Declaración de Prácticas de Certificación correspondiente. La revocación y caducidad del certificado supone en todos los casos la destrucción de las claves asociadas. **[DEL-6.3.2-02]**

4.5.1.4. Copia de seguridad y restauración de la claves de firma

Las claves de los firmantes están protegidas por la clave maestra del módulo criptográfico, sólo se pueden utilizar cuando el módulo criptográfico está activo.

Cuando se realiza una copia de seguridad de las claves de los firmantes se utiliza el algoritmo de cifrado AES y una longitud de clave de 128 bits. **[GEN-6.3.3-01] [GEN-6.3.3-02]**

Se mantienen copias de seguridad periódicas de la base de datos del SSA, donde se encuentran referenciadas las claves de los firmantes, y del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente.

Las claves de infraestructura del SSASC son siempre almacenadas en contenedores cifrados.

El módulo criptográfico que contiene la clave maestra del SSASC que protege las claves de todos los firmantes requiere de control dual para su operación, copia de seguridad y restauración. La clave maestra del SSASC nunca abandona el módulo criptográfico en claro. **[GEN-6.3.3-03]**

El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio. **[GEN-6.3.3-04]**

4.5.2 Uso de certificados y claves públicas de parte que confía

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

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

4.6 Renovación del certificado (sin cambio de claves)

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

4.6.1 Circunstancia para la renovación del certificado

Sin estipulación.

4.6.2 Quién puede solicitar la renovación

Sin estipulación.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Sin estipulación.

4.6.4 Notificación al suscriptor de la emisión de un nuevo certificado

Sin estipulación.

4.6.5 Conducta que constituye la aceptación de un certificado de renovación

Sin estipulación.

4.6.6 Publicación del certificado de renovación por parte de la CA

Sin estipulación.

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

Sin estipulación.

4.7 Renovación del certificado con cambio de clave

4.7.1 Circunstancia para el cambio de clave del certificado

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

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

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

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

4.7.3 Procesamiento de solicitudes de cambio de claves de certificados

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

4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado

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

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

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

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

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

4.8 Modificación del certificado

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

4.8.1 Circunstancia para la modificación del certificado

Sin estipulación.

4.8.2 Quién puede solicitar la modificación del certificado

Sin estipulación.

4.8.3 Procesamiento de solicitudes de modificación de certificados

Sin estipulación.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

Sin estipulación.

4.8.5 Conducta que constituye la aceptación del certificado modificado

Sin estipulación.

4.8.6 Publicación del certificado modificado por la CA

Sin estipulación.

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

Sin estipulación.

4.9 Revocación y suspensión de certificados

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

4.9.1 Circunstancias para la revocación

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

4.9.2 Quién puede solicitar la revocación

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

4.9.3 Procedimiento de solicitud de revocación

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

4.9.4 Periodo de gracia de la solicitud de revocación

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

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

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

4.9.6 Requisito de verificación de revocación para las partes que confían

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

4.9.7 Frecuencia de emisión de CRL

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

4.9.8 Latencia máxima para las CRL

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

4.9.9 Disponibilidad de verificación de estado / revocación en línea

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

4.9.10 Requisitos de verificación de revocación en línea

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

4.9.11 Otras formas de anuncios de revocación disponibles

SIn estipulación.

4.9.12 Requisitos especiales relacionados con el compromiso clave

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

4.9.13 Circunstancias para la suspensión

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

4.9.14 Quién puede solicitar la suspensión

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

4.9.15 Procedimiento de solicitud de suspensión

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

4.9.16 Límites del período de suspensión

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

4.10 Servicios de estado de certificados

4.10.1 Características operativas

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

4.10.2 Disponibilidad del servicio

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

4.10.3 Funciones opcionales

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

4.11 Finalización de la suscripción

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

4.12 Custodia y recuperación de claves

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

4.12.1 Política y prácticas de custodia y recuperación de claves

Sin estipulación.

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

Sin estipulación.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de seguridad física

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 procedimientos

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

5.2.1 Roles de confianza

El SSA implementa los siguientes roles de gestión:

- Responsable de seguridad (security officer): tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.
- Administrador del sistema (system administrators): es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.
- Operador del sistema (system operators): es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.
- Auditor del sistema (system auditor): está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

Firmaprofesional asigna estos roles a personal cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1.

[OVR-6.5.1-01]

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 autentificación 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

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

5.4. Procedimientos de auditoría de seguridad

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional. **[OVR-6.4.5-01] [OVR-6.4.5-02]**

El SSASC guarda registro, al menos, de los siguientes eventos:

- Inicialización de sistema, arranque, parada y cambios de configuración.
- Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción)
- Uso de claves de los firmantes.
- Autenticación de los firmantes (incluyendo intentos fallidos).
- Gestión de los datos de activación de firma del firmante (cambios de PIN)
- Arranque y parada de las funciones de auditoría.
- Cambio de la configuración de las funciones de auditoría.
- Accesos al sistema por parte de los usuarios administradores.

El SSAC deja de procesar de forma automática peticiones en el caso de que sus funciones de auditoría no estén disponibles. **[OVR-6.4.5-03]**

El SSAC genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores.

El SSAC protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando un índice único de registro. **[OVR-6.4.5-04]**

Todos los registros de eventos del registro de auditoría del SSA incluyen la siguiente información:

- Fecha y hora del evento.
- Tipo de evento.

- Identidad de la entidad (firmante, administrador o proceso) responsable de la acción.
- Resultado del evento (éxito o error) **[OVR-6.4.5-05]**

El SSASC comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSA dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema. **[OVR-6.4.5-06]**

Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP utilizando como referencia el ROA (Real Observatorio de la Armada). Existen controles para detectar problemas que puedan comprometer la sincronización. **[OVR-6.4.5-07]**

5.5. Archivo de informaciones

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional. **[OVR-6.4.6-01]**

5.6. Cambio de claves

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

5.7. Compromiso de claves y recuperación de desastre

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

5.8 Cese de actividad

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

6 Controles de seguridad técnica

6.1. Operaciones y sistemas

La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC. **[OVR-6.5.2-01]**

El componente software SSA y el módulo HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos en la Declaración de Seguridad de su certificación Common Criteria. **[OVR-6.5.2-02] [GEN-A.4-02] [GEN-A.5-02]**

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

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

6.3. Otros aspectos de la gestión del par de claves

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

6.4. Datos de activación

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional.

6.5. Controles de seguridad informática

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional. **[OVR-6.5.3-01]**

El SSASC se encuentra monitorizado y se generan alertas que son enviadas a los administradores del sistema cuando se detectan eventos que pueden impactar en su disponibilidad o comprometer su seguridad **[OVR-6.5.3-02]**

Adicionalmente el sistema de monitorización permite generar alertas basadas en reglas de correlación para detectar comportamientos que pueden denotar un potencial ataque.

6.6. Controles técnicos del ciclo de vida

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional. [**OVR-6.5.4-01]**

6.7.Controles de seguridad de red

Ver apartado correspondiente en la Declaración de Prácticas de Certificación de Firmaprofesional. **[OVR-6.5.5-01]**

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 el presente documento se emiten los siguientes tipos de certificados, con sus OID asociados:

Tipo de Certificado	OID
Certificados Corporativos de Colegiado. Nivel alto con DCCF centralizado	1.3.6.1.4.1.13177.10.1.1.3
Certificados Corporativos de Persona Física. Nivel alto con DCCF centralizado	1.3.6.1.4.1.13177.10.1.2.3
Certificados Corporativos de Representante Legal. En DCCF centralizado	1.3.6.1.4.1.13177.10.1.11.3
Certificados Corporativos de Representante Voluntario frente a las Administraciones Públicas. En DCCF centralizado.	1.3.6.1.4.1.13177.10.1.12.3
Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica. En DCCF centralizado	1.3.6.1.4.1.13177.10.1.13.3
Certificados de Empleado Público. Nivel Alto con DCCF centralizado	1.3.6.1.4.1.13177.10.1.22.3
Certificados Personales. En DCCF centralizado	1.3.6.1.4.1.13177.10.1.40.3

7.1.7 Uso de la extensión Policy Constraints

Sin estipulación.

7.1.8 Sintaxis y semántica de los calificadores de política

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

7.1.9 Semántica de procesamiento de la extensión critical Certificate Policies

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

7.2 Perfil CRL

7.2.1 Número(s) de versión

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

7.2.2 Extensiones de CRL y entradas de CRL

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

7.3 Perfil OCSP

7.3.1 Número(s) de versión

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

7.3.2 Extensiones OCSP

Sin estipulación.

8. Auditorías de cumplimiento y otros controles

8.1 Frecuencia de las auditorías

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

8.2 Cualificación del auditor o evaluador

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

8.3 Relación entre el auditor y la autoridad auditada

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

8.4 Aspectos cubiertos por la evaluación

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

8.5 Acciones a emprender como resultado de la detección de deficiencias

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

9. Otras cuestiones legales y de actividad

9.1 Tarifas

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

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

9.1.1 Tarifas de emisión o renovación de certificados

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

9.1.2 Tarifas de acceso a los certificados

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

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

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

9.1.4 Tarifas por otros servicios

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

9.1.5 Tarifas de reembolso

Sin estipulación.

9.2 Responsabilidades económicas

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

9.2.1 Cobertura del seguro

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

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro o garantía para las entidades finales

Sin estipulación.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

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

9.3.2 Información no confidencial

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

9.3.3 Responsabilidad de proteger la información confidencial

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

9.4 Protección de la información personal

9.4.1 Política de protección de datos de carácter personal

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

9.4.2 Información tratada como privada

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

9.4.3 Información no considerada privada

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

9.4.4 Responsabilidad de proteger la información privada

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

9.4.5 Aviso y consentimiento para el uso de la información privada

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

9.4.6 Divulgación en virtud de un proceso judicial o administrativo

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

9.4.7 Otras circunstancias de divulgación de información

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

9.5 Derechos de propiedad intelectual

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

9.6 Obligaciones y garantías

9.6.1 Obligaciones de la AC

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

9.6.2 Obligaciones de la AR

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

9.6.3 Obligaciones de los solicitantes

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

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

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

9.6.5 Declaraciones y garantías de otros participantes

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

9.7 Exención de garantía

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

9.8 Limitaciones de responsabilidad

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

9.9 Indemnizaciones

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

9.10 Periodo de validez y terminación

9.10.1 Plazo

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

9.10.2 Terminación

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

9.10.3 Efecto de la terminación y supervivencia

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

9.11 Avisos y comunicaciones individuales con los participantes

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

9.12 Modificaciones o cambios en las especificaciones

9.12.1 Procedimiento para los cambios

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

9.12.2 Mecanismo y plazo de notificación

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

9.12.3 Circunstancias en las que debe modificarse la OID

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

9.13 Disposiciones para la resolución de conflictos

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

9.14 Normativa aplicable

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

9.15 Cumplimiento de la normativa aplicable

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

9.16 Disposiciones diversas

9.16.1 Acuerdo completo

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

9.16.2 Independencia

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

9.16.3 Resolución por vía judicial

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

9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)

Sin estipulación.

9.16.5 Fuerza mayor

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

9.17 Otras disposiciones

Sin estipulación.

firmaprofesional