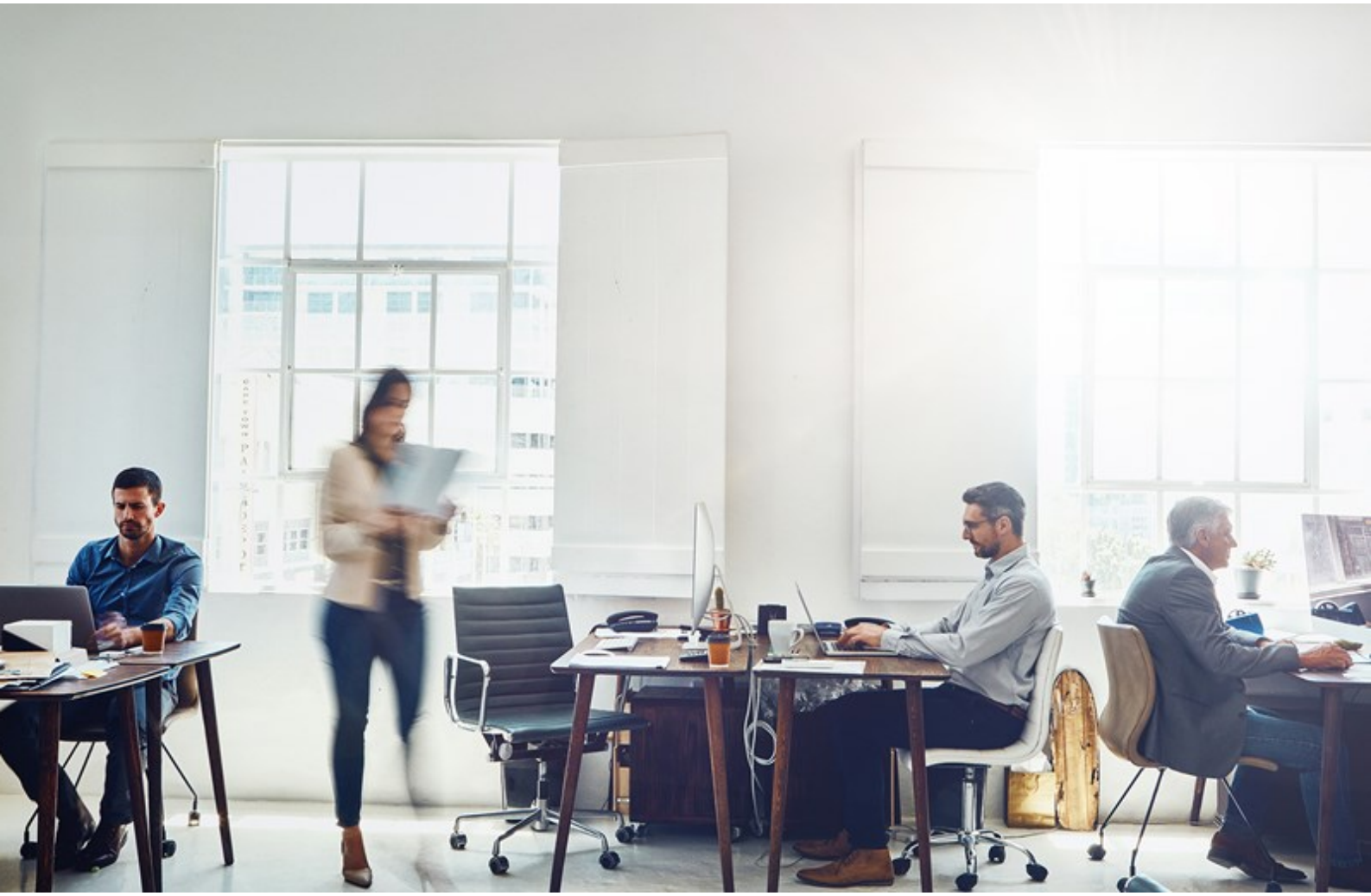
firmaprofesional

Documentación General

Declaración de Prácticas de Certificación (CPS) de Firmaprofesional, S.A.

Versión: 240520

Clasificación: Público



BARCELONA
PASSEIG DE GRÀCIA 50, 2-1
08007 BARCELONA
+34 934 774 245

MADRID
CALLE CANTABRIA 5 (Ed. Amura)
28108 ALCOBENDAS
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Histórico de versiones

Versión	Sección y cambios	Fecha de Publicación
6.1	*(para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com)*	20/10/2014
151005	● "*1.3.2 Autoridad de Certificación (CA)*": ○ Limitación de CA Subordinadas a las que se puede emitir certificados. ○ Limitación de CAs que pueden emitir certificados SSL, SSL EV o asimilables. ○ Adición de identificación, aclaraciones e incorporación de restricciones técnicas, de certificados SHA2 para las siguientes CAs: ■ Autoridad de Certificacion Firmaprofesional CIF A62634068 ■ AC Firmaprofesional – INFRAESTRUCTURA ■ AC Firmaprofesional – CFEA ■ AC Firmaprofesional – OTC ■ SIGNE Autoridad de Certificacion ■ SEU Autoridad de Certificacion ■ Santander Digital Signature ● "*1.4.3* Certificados *para la Administración Pública*": eliminado el certificado de Sede Electrónica, que se traslada a la sección "Certificados de Servicio Seguro", por coherencia funcional. ● "*2.1 Repositorios*": actualizada la tabla ● "*5.8.2 Autoridad de Registro*":añadida la obligación a la RA de entregar toda la documentación a Firmaprofesional. ● "*6.1.5 Tamaño de las claves*": dada la diversidad de políticas de certificado se abre la definición del período de validez para los certificados de entidad final.	05/10/2015
160229	● "*1.4.3 Certificados para la Administración Pública*": aclarada la naturaleza de los certificados de Sede Electrónica ● "*1.3.2.2 Autoridades de Certificación Subordinadas Públicas*": incluidos los certificados de "Sede Electrónica" como emitidos por la CA AC FIRMAPROFESIONAL - INFRAESTRUCTURA. ● Eliminada la referencia explícita a la versión de la "Mozilla CA Certificate Inclusion Policy" y de "Baseline Requirements	29/02/2016

	Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates", referenciando a "la versión vigente".	
171121	• "*5.3.5 Frecuencia y secuencia de rotación de tareas*": creado apartado. • Se revisa todo el documento a partir de la revisión eIDAS. • Se cambia Dispositivo Seguro por Dispositivo Cualificado. Se eliminan referencias a la ley 11/2007. • Se indica la revocación de los certificados de la Autoridad de Certificación Subordinada del PSC SEU. • Eliminación del OID de firma de código.	21/11/2017
180704	• Inclusión de Certificados Corporativos de Representante de Entidad sin Personalidad Jurídica. • Verificación de adherencia a Mozilla Root Store Policy, version 2.5. • Inclusión de tratamiento de compromiso de suite criptográfica. • Eliminación de la sección certificados Corporativos de uso restringido y de los certificados de Infraestructura, de firma de código y de factura electrónica. • "*1.4.7. Solicitud de kit de certificados de prueba*": creado apartado. • "*1.5.1. Notificación de usos no autorizados, quejas o sugerencias*": creado apartado. • Inclusión de datos de certificado SHA256 de la Autoridad de Certificación Subordinada AC Firmaprofesional - AAPP. • Eliminación de referencias a Firma Electrónica Avanzada.	04/07/2018
181221	• "*1.4. Usos no autorizados de los certificados*": eliminación de tipos de certificados. • Comunicación de revocación de los certificados de CA de Banco Santander • Eliminación de la posibilidad de consentir la publicación en los repositorios de los certificados. • Actualización a requerimientos de CA/Browser -Forum V.1.6.1 de octubre de 2018 en la sección 4.9 • Actualización de referencias de la legislación en materia de Protección de Datos Personales. Eliminación del fichero inscrito	21/12/2018

	en la AEPD por la supresión del Registro de la AEPD. • Comunicación de revocación de certificados de CA CFEA y OTC y nueva emisión de los mismos con nuevas restricciones técnicas. • Comunicación de revocación de certificado de CA INFRAESTRUCTURA con hash SHA1. • Se añade la Entidad participante "Punto de Verificación Presencial" • El periodo de validez del certificado de operador pasa a ser de 1 a 5 años	
190612	• Revocación de uno de los certificados de la CA INFRAESTRUCTURA. • Verificación de adherencia a Mozilla Root Store Policy, version 2.6.1. • Adición de condiciones de revocación de certificados para PSD2. • Adición de normativa de PSD2 aplicable. • "*4.4.2. Publicación del certificado*": añadido párrafo por emisión de certificados para PSD2.	12/06/2019
190806	• Reestructuración de puntos del histórico de versiones. • "*3.2.7. Identificación de certificados de alto riesgo*": creado apartado. • "*4.4. Aceptación del certificado*" (exclusivo en la versión en castellano): modificado el nivel del título, que pasa de nivel 3 a nivel 2. Inicialmente era "4.3.3. Aceptación del certificado". • "*4.9.9. Requisitos de comprobación de revocación en línea*": añadidas consideraciones para el uso del servicio OCSP. • "*5.4.7. Análisis de vulnerabilidades*": indicado el tipo de análisis de vulnerabilidades realizado. • "*6.2.6. Transferencia de la clave privada a o desde el módulo criptográfico*": reestructuración del apartado. • "*9.14. Normativa aplicable*": incluida adhesión a la última versión de los "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"	06/08/2019
200205	• "*8.4.1. Auditoría en las Autoridades de Registro*": eliminado la	05/02/2020

	explicitación sobre la realización de auditorías por terceros. • Adaptación a los requerimiento de la última versión de la Política de Mozilla Root Store • Adición de OID 24 = Empleado Público Autenticación nivel alto	
200417	• Trasladado de las verificaciones del registro CAA de la sección 3.2.2 a la sección 4.2 • Introducción de la identificación por videoconferencia en el apartado 3.2.3	17/04/2020
200806	• Procedimiento de generación de la última CRL en caso de compromiso de claves o finalización del servicio. Sección 4.10 • Se añaden nuevas versiones de los certificados de CA subordinada INFRAESTRUCTURA, CFEA, OTC y SIGNE. Sub secciones de 1.3.2 Autoridad de certificación (CA)	06/08/2020
201001	• Sustitución del término PVP por Entidades Solicitantes • Incorporación en sección 3.2 tabla de registro de fuentes de verificación.	01/10/2020
210217	• Revisión de la alineación de la estructura del documento con la RFC 3647 • Adaptación a la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza • Actualización de certificados de la jerarquía	17/02/2021
210322	• Actualización de certificados de la jerarquía	22/03/2021
210628	• Actualización de certificados de la jerarquía Timestamp 2021 • Actualización del apartado 1.4.2.1. y 1.5.2. incorporando compromiso de clave, quejas o sugerencias • Actualización apartado 2.4 referencia Auditorías BR. • Actualización apartado 3.1.4 referencia EV Guidelines y requisitos datos de personas físicas o jurídicas sin restricción de caracteres. • Actualización apartado 3.2 criterios de selección de Fuentes de Verificación. • Actualización apartado 3.2.2.1 referencia a la PC de autenticación Web • Actualización apartado 3.2.4 y 3.2.7 • Actualización apartado 4.2 referencia RFC 6844 ERRATA 5065 • Actualización apartado 4.9.1 incorporación de nuevas circunstancias de revocación • Actualización de apartado 4.9.3.1 Procedimiento online	28/06/2021

	• Actualización del apartado 4.9.12 métodos de comprobación de compromiso de claves • Actualización del apartado 6.2.1 • Actualización del apartado 4.10.2 • Actualización del apartado 5.3.1 requisitos de formación específica de los especialistas de validación • Actualización del apartado 5.3.7 • Actualización apartado 5.7.3 Notificación fabricantes software por compromiso de claves. • Actualización apartado 6.1.7 usos admitidos de las claves aclarando los usos permitidos de los certificados • Actualización apartado 6.2.1 Pérdida de cualificación de QSCD • Actualización apartado 6.7. • Actualización apartado 7.1.3 incorporación de fecha de prohibición de uso de SHA1 • Actualización apartado 9.2.1 aclaración cobertura exigida por las EV Guidelines • Actualización apartado 9.5 • Actualización apartado 9.14 y 9.15 prevalencia de las EV Guidelines y solución de conflictos con la ley nacional	
220413	• Actualización de certificado de la jerarquía Secure Web 2022 y Roots de Nueva Jerarquía • Incorporación referencia OID Perfil Corporativo de Persona Física CON email protection apartado 1.2.2. • Actualización apartado 2.1 crls nuevas CAs y SubCAs y 7.1 • Sustitución referencia RFC 6844 • Actualización apartado 6.1.5 y 6.1.6 • Actualización apartado 3.1.4 y 3.2.3 • Actualización apartado 4.3.1, 4.4.1 y 4.10.2 • Actualización apartado 4.9.7 Certificados caducados no aparecen en la CRL • Actualización 9.6.4 • Actualización del apartado 1.5.3. Previsión en la CPS del intervalo de revisión de la Política de Seguridad. Adaptación a la ETSI 319 401 V2.3.1	13/04/2022
220623	• Actualización apartado 1.3.1.3 Incorporación Nuevas SubCAs (NOQ B3, B4 y B5) • Actualización apartado 4.9.7 • Actualización apartado 6.2.1 y 9.2.1	23/06/2022
221220	• Actualización apartado 1.3.1.3 Incorporación Nuevas SubCAs (A1, A2, B1, B2 y Root-A Web Cross)	20/12/2022

	• Incorporación del Hash SHA256 en todas las CAs Root y SubCAs • Actualización apartado 2.1 • Modificación apartado 5.7.3 LastCRL en caso de compromiso de claves de la CA. • Inclusión de Fecha de destrucción de claves SubCA Secure Web 2020	
230413	• Actualización apartado 4.9.1 • Actualización apartado 5.4.8 • Actualización apartado 6.2.1 • Precisión apartado 5.2.1	13/04/2023
240520	• Actualización apartado 1.3.1.2 y 2.1 por incorporación Nueva SubCA • Actualización apartados 3.2.5 / 4.2.1 / 4.2.2 / 4.7.3 / 4.9.3.1 / 7.1.2 / 7.1.4 • Actualización ubicación nuevas oficinas en apartado 1.5.2 y página inicial. • Actualización apartado 1.3.1.5 de CA's caducadas • Actualización referencia en apartado 1.1 • Actualización definición en 1.3.3.2	20/05/2024

Índice

1 Introducción

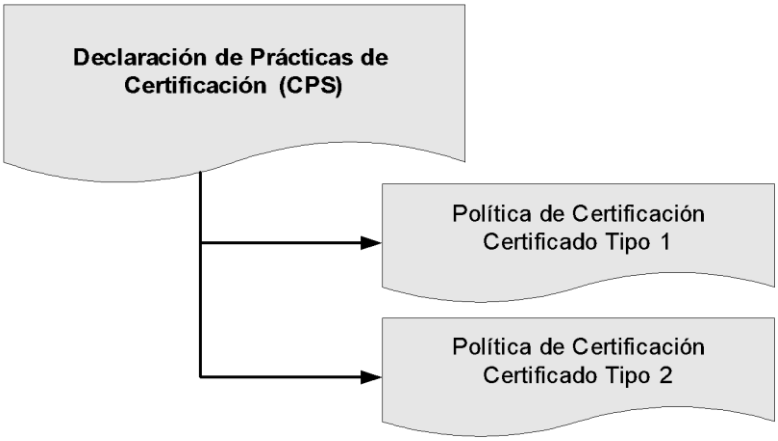
1.1 Presentación

Firmaprofesional S.A. nació como un proyecto de diversos Colegios Profesionales y se constituyó como Sociedad Anónima en el año 2001 con el fin de actuar con total independencia como Prestador de Servicios de Certificación (PSC) que emite certificados cualificados según la Ley 6/2020 de 11 de noviembre reguladora de determinados aspectos de los servicios electrónicos de confianza.

La Ley 6/2020, de 11 de noviembre , reguladora de determinados aspectos de los servicios electrónicos de confianza exige a los prestadores de servicios de certificación efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada Declaración de Prácticas de Certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. El presente documento tiene como objetivo cumplir con estos requisitos establecidos por la Ley, constituyéndose como la **Declaración de Prácticas de Certificación** de Firmaprofesional, (en inglés CPS o *Certification Practice Statement*)

La estructura de este documento está basada en la especificación del estándar "RFC3647 - *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*", creado por el grupo de trabajo PKIX del IETF.

Adicionalmente a los términos y condiciones establecidos en esta CPS, cada tipo de certificado emitido por Firmaprofesional se rige por las condiciones contenidas en el "**Texto de Divulgación**" (en inglés PDS o *PKI Disclosure Statement*), además de los requerimientos que se encuentran en la "**Política de Certificación"** (en inglés CP o *Certificate Policy*).



Firmaprofesional adecua sus servicios de certificación al Reglamento (UE) 910/2014 del Parlamento Europeo 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 y por la que se deroga la Directiva 1999/93/CE.

Firmaprofesional adecua sus servicios a las siguientes normas ETSI de referencia:

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures)
- ETSI EN 319 412-2 (Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons)
- ETSI EN 319 412-3 (Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons)
- ETSI EN 319 412-4 (Certificate Profiles; Part 4: Certificate profile for web site certificates)
- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)
- ETSI TS 119 495 (Certificate Profiles and TSP Policy Requirements for Open Banking)

1.2 Nombre del documento

1.2.1 Identificación

Nombre:	Declaración de Prácticas de Certificación (CPS)
Versión:	240520
Descripción:	Declaración de Prácticas de Certificación de Firmaprofesional S.A.
Fecha de Emisión:	20/05/2024
OID	1.3.6.1.4.1.13177.10.0.230413
Localización	https://www.firmaprofesional.com/cps

1.2.2 OIDs

Siguiendo los estándares de certificación digital, Firmaprofesional utiliza Identificadores de Objetos (OID) definidos en el estándar ITU-T Rec. X.660 (2004) | ISO/IEC 9834-1:2005 "Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs".

Firmaprofesional tiene registrado en IANA el número "13177" como OID de empresa privada (http://www.iana.org/assignments/enterprise-numbers).

El significado de los OID que comienzan por "1.3.6.1.4.1.13177" es el siguiente:

OID	Tipo de Objeto	Descripción
10.0.AAMMDD	Declaración de Prácticas de Certificación (CPS)	Versión del documento.

10.1.T.D	Políticas de Certificación	T = Tipo de Certificado 1 = Corporativo de Colegiado 2 = Corporativo de Persona Física 3 = Servidor Web SSL y PSD2 4 = Servicio Seguro TSA 5 = Corporativo de Persona Jurídica 6 = Corporativo de Factura Electrónica 10 = Corporativo de Sello Empresarial y PSD2 11 = Corporativo de Representante Legal 12 = Corporativo de Representante Voluntario 13 = Corporativo de Representante de Entidad Sin Personalidad Jurídica 20 = Sede Electrónica 21 = Sello de Órgano 22 = Empleado Público 23 = Empleado Público con Seudónimo 24 = Empleado Público Autenticación nivel alto 30 = Certificado de Infraestructura 31 = Servicio Seguro VA 40 = Certificado Personal D = Dispositivo / Nivel de Seguridad 1 = DCCF portable (Nivel Alto) o SSL-OV o para servicio cualificado (aplica a Servicio Seguro VA o TSA) 2 = Otros dispositivos (Nivel Medio) o para servicios no cualificados (aplica a Servicio Seguro VA o TSA) 3 = DCCF centralizado 10 = SSL EV y PSD2
10.10.N	Política de Certificado de CA Subordinada	1 = CA Subordinada Cualificada 2 = CA Subordinada No Cualificada
20.0.1	Política de Servicio no cualificado de Sellado de Tiempo	
0.4.0.2023.1.1	Política de Servicio cualificado de Sellado de Tiempo (según ETSI EN 319 421)	Este OID no lleva el prefijo 1.3.6.1.4.1.13177, que identifica a Firmaprofesional

1.3 Entidades Participantes

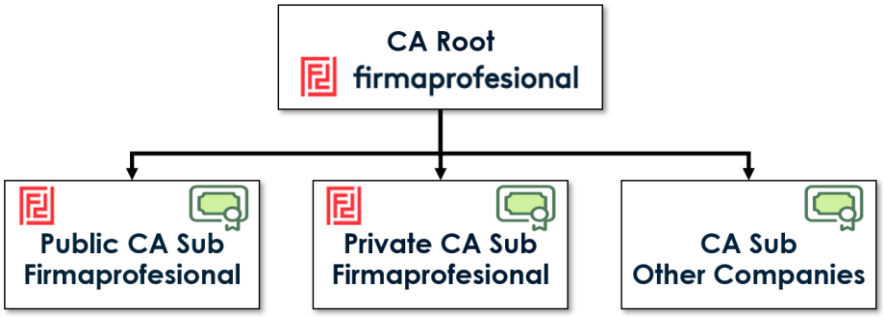
Firmaprofesional es un Prestador de Servicios de Confianza (PSC) que emite certificados cualificados según la Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza..

Firmaprofesional es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida de los certificados. Las funciones de autorización, registro, emisión y revocación respecto de los certificados personales de entidad final, pueden ser realizadas por Autoridades de Registro que Firmaprofesional haya contratado y formado al personal que vaya a realizar dichas funciones.

Firmaprofesional también ofrece servicios de validación de firmas electrónicas y de sellado de tiempo, regidos por sus políticas particulares, no incluidas en este documento

1.3.1 Autoridad de Certificación (CA) Prestador de Servicios de Confianza (PSC)

Hasta el año 2022, el sistema de certificación de Firmaprofesional ha estado compuesto por diversas Autoridades de Certificación (en inglés CA o Certificate Authority) organizadas bajo una Jerarquía de Certificación de dos niveles, formada por una única CA Raíz y por diversas CA Subordinadas.



En 2022 se emiten 3 nuevas CAs Raíz con algoritmo de firma ecdsa-with-SHA384.

Las CA's subordinadas pueden estar emitidas a nombre de Firmaprofesional o a nombre de otros PSC. En cualquier caso, todas las CAs que forman parte de la Jerarquía de Certificación de Firmaprofesional deben ser operadas técnicamente por Firmaprofesional en las infraestructuras de Firmaprofesional.

No se autoriza la posibilidad de que Firmaprofesional emita un certificado de CA Subordinada para un PSC que opere la PKI con sus propios medios o con su propia infraestructura. De tal manera que Firmaprofesional garantiza que la seguridad técnica de todas las CAs subordinadas es equivalente, independientemente de la entidad que aparezca como PSC.

En el caso de que un PSC desee operar la PKI con sus propios medios o con su propia infraestructura, se deberá revocar la CA Subordinada y crear otra CA fuera de la Jerarquía de Firmaprofesional.

Firmaprofesional puede operar otras PKI fuera de la Jerarquía de Firmaprofesional.

1.3.1.1 CAs Raíz

Se denomina Autoridad de Certificación Raíz (CA Root) a la entidad dentro de la jerarquía que emite certificados a otras autoridades de certificación, y cuyo certificado de clave pública ha sido autofirmado. Su función es firmar el certificado de las otras CAs pertenecientes a la Jerarquía de Certificación.

1.3.1.1.1 Autoridad de Certificacion Firmaprofesional CIF A62634068

Se dispone de dos versiones de este certificado, ambas con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y otra con el algoritmo SHA2.

Los datos de identificación del Certificado Raíz de Firmaprofesional son:

- CN: Autoridad de Certificacion Firmaprofesional CIF A62634068
- Hash SHA1: AEC5 FB3F C8E1 BFC4 E54F 0307 5A9A E800 B7F7 B6FA
- Hash SHA256: 04048028BF1F2864D48F9AD4D83294366A828856553F3B14303F90147F5D40EF
- Válido desde el 20 de mayo de 2.009 hasta el 31 de diciembre de 2.030
- Tipo de clave: RSA 4096 bits – SHA1

- CN: Autoridad de Certificacion Firmaprofesional CIF A62634068
- Hash SHA1: 0bbe c227 2249 cb39 aadb 355c 53e3 8cae 78ff b6fe
- Hash SHA256: 57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A
- Válido desde el 23 de septiembre de 2.014 hasta el 5 de mayo de 2.036
- Tipo de clave: RSA 4096 bits – SHA256

Ambos certificados CA Raíz se pueden utilizar conjuntamente e indistintamente ya que todos los certificados emitidos por Firmaprofesional validan frente a ambos certificados.

Desde diciembre de 2016 Firmaprofesional solo emite certificados en SHA256.

En 2022 se emitieron 3 CAs Raíz con algoritmo de firma ecdsa-with-SHA384. Los datos de identificación de las nuevas CAs Raíz de Firmaprofesional emitidas son:

1.3.1.1.2 FIRMAPROFESIONAL CA ROOT-A WEB

- CN: FIRMAPROFESIONAL CA ROOT-A WEB
- Hash SHA1: A8:31:11:74:A6:14:15:0D:CA:77:DD:0E:E4:0C:5D:58:FC:A0:72:A5
- Hash SHA256: BE:F2:56:DA:F2:6E:9C:69:BD:EC:16:02:35:97:98:F3:CA:F7:18:21:A0:3E:01:82:57:C5:3C:65:61:7F:3D:4A
- Válido desde el 6 de Abril de 2.014 hasta el 31 de Marzo de 2047
- Tipo de clave: SHA384 WITH ECDSA

1.3.1.1.3 FIRMAPROFESIONAL CA ROOT-B GP

- CN: FIRMAPROFESIONAL CA ROOT-B GP
- Hash SHA1: 79:5B:1E:B8:C3:ED:9F:0D:8C:73:67:59:95:7D:BA:53:1C:69:D7:73
- Hash SHA256: 72:21:C0:A1:66:8F:4A:38:F1:FA:98:9D:DD:AB:61:A8:C0:EC:71:F3:26:82:C7:CD:01:83:E0:A2:D7:29:AE:FD
- Válido desde el 6 de Abril de 2.014 hasta el 31 de Marzo de 2047
- Tipo de clave: SHA384 WITH ECDSA

1.3.1.1.4 FIRMAPROFESIONAL CA ROOT-C LATAM

- CN: FIRMAPROFESIONAL CA ROOT-C LATAM
- Hash SHA1: 3B:3F:65:25:3E:21:C2:2A:70:2F:8E:92:94:FD:F2:B6:C9:D7:E7:07
- Hash SHA256: 42:7D:9B:78:10:B3:7A:6F:6B:9C:6D:60:28:C0:81:32:FF:88:44:BE:07:68:C0:B8:9D:CE:8B:DA:B3:18:6C:00
- Válido desde el 6 de Abril de 2.014 hasta el 31 de Marzo de 2047
- Tipo de clave: SHA384 WITH ECDSA

1.3.1.2 Autoridades de Certificación Subordinadas Públicas

Se denomina Autoridades de Certificación Delegadas o Subordinadas (CASub) a las entidades dentro de la jerarquía de certificación que emiten certificados de entidad final y cuyo certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz.

Las autoridades de certificación subordinadas públicas emiten certificados que pueden ser utilizados públicamente. Estos certificados están regulados por distintos organismos (ej. Ministerio de Asuntos Económicos y Transformación Digital), reconocidos por distintas plataformas (ej, Microsoft, Firefox, Chrome, Apple, Adobe, @Firma, PSIS o AEAT) y auditados por distintas normas (ej. Webtrust).

1.3.1.2.1 AC Firmaprofesional - CA1

La Autoridad de Certificación Subordinada "AC Firmaprofesional - CA1" emite certificados digitales a Corporaciones Privadas, conforme a lo establecido en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza:

- CN = AC Firmaprofesional - CA1
- Hash SHA1: A366 C03C D7CB 1D13 90DE EBB9 67DF 588B 1A4E BFDE
- Hash SHA256: 0EBBDF146E63F70FAA5927EE8E5346E9C96C5F0D9BDD3212B04ED6687179874D
- Válido desde el 25 de agosto de 2.009 hasta el 16 de junio de 2.030
- Tipo de clave: RSA 2048 bits – SHA1

1.3.1.2.2 AC Firmaprofesional - CUALIFICADOS

La Autoridad de Certificación Subordinada "AC Firmaprofesional - CUALIFICADOS" emite certificados digitales cualificados conforme a lo establecido en la Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Esta CA está adaptada a los requerimientos del "Reglamento (UE) No 910/2014 del Parlamento Europeo 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 y por la que se deroga la Directiva 1999/93/CE (eIDAS)" y está emitida con el algoritmo SHA256.

Se dispone de dos versiones de este certificado, ambas con el mismo par de claves y los mismos datos de identificación y fin de vigencia. Su única diferencia radica en que la versión más reciente tiene codificado en UTF8 el campo Issuer para mejorar la compatibilidad:

- CN = AC Firmaprofesional - CUALIFICADOS
- Hash SHA1: 3486 ED23 6221 5545 9E9B 25FF 3F21 AD76 2798 7387
- Hash SHA256: 2B75CC4F36759CFC4C6637B1E0E54359457DB57E74DE4D2DC5D02CDDFF2960CF
- Válido desde el 18 de septiembre de 2014 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA-256

- CN = AC Firmaprofesional - CUALIFICADOS
- Hash SHA1: 9F2B E8F3 E159 2F2F EC2C 6C88 A1C2 1579 286F 5CE8
- Hash SHA256: 4CCF17C0C8C1C10D5876EC5E3280FE8D134DF36AEDD8444289B990BC3741E74F
- Válido desde el 14 de diciembre de 2018 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits - SHA-256

1.3.1.2.3 FIRMAPROFESIONAL ICA B01 QUALIFIED 2022

La Autoridad de Certificación Subordinada "FIRMAPROFESIONAL ICA B01 QUALIFIED 2022" emitirá certificados digitales para servicios de firma electrónica y sello electrónico cualificados.

- CN = FIRMAPROFESIONAL ICA B01 QUALIFIED 2022
- Hash SHA1: 8A:1E:7F:F9:C7:40:D2:D6:24:09:E9:F7:66:2B:0F:0F:D2:7F:DB:AE
- Hash SHA256: 4A:86:F3:33:7C:EC:89:A6:78:96:B8:A6:CB:BA:DA:84:AC:18:1E:B0:09:67:9E:15:04:15:6C:34:BC:9F:8A:A1
- Válido desde el 19 de julio de 2022 hasta el 31 de marzo de 2047
- Tipo de Clave: SHA384 WITH ECDSA

1.3.1.2.4 AC Firmaprofesional – INFRAESTRUCTURA

La Autoridad de Certificación Subordinada "AC Firmaprofesional – INFRAESTRUCTURA" emite certificados digitales para securizar las comunicaciones y servicios mediante protocolos criptográficos compatibles con la tecnología PKI.

Todos los certificados SSL, SSL EV y de Sede Electrónica emitidos bajo la Jerarquía de Certificación de Firmaprofesional deben ser emitidos por esta CA. Por lo tanto, desde ninguna otra CA de la Jerarquía de Certificación de Firmaprofesional, ya sea pública, privada o subordinada de otros PSC se podrán emitir certificados SSL, SSL EV o de Sede Electrónica.

Se dispone de las siguientes versiones de este certificado, todos ellos con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y el resto el algoritmo SHA2. Éstas segundas están restringida técnicamente mediante el uso de la extensión Extended Key Usage (EKU – extKeyUsage) según lo establecido en los Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates y Mozilla CA Certificate Inclusion Policy vigentes en el momento de entrada en vigor de la presente CPS.

- CN = AC Firmaprofesional – INFRAESTRUCTURA
- Hash SHA1: d52f 537f 62ce 24d0 6fb5 9b0a 02bf c4a8 f7c1 6b66
- Hash SHA256: 376DA371D590FED38A0D47BCBAE142B04A510373D2976A69348AD1C160F889A0
- Válido desde el 18 de junio de 2013 hasta el 31 de Diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA1
- Fecha de revocación: 13 de abril de 2018

- CN = AC Firmaprofesional – INFRAESTRUCTURA
- Hash SHA1: ac 1e 38 0a 14 dd d2 22 81 0d db f4 cf 32 0f 1a fe 91 09 40
- Hash SHA256: CD74198D4C23E4701DEA579892321B9E4F47A08BD8374710B899AAD1495A4B35
- Válido desde el 29 de julio de 2015 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Firma de código (1.3.6.1.5.5.7.3.3)
  - Impresión de fecha (1.3.6.1.5.5.7.3.8)
  - Firma de OCSP (1.3.6.1.5.5.7.3.9)
- Fecha de revocación: 11/11/2020

- CN = AC Firmaprofesional - INFRAESTRUCTURA
- Hash SHA1: 2dace5f67c666315e50457fd468d2a5744ed882a
- Hash SHA256: 48C03AB647D5BD7E0D0C43C0B5D674CC9893F836AB863AF8F3F1384B544D833
- Válido desde el 9 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Impresión de fecha (1.3.6.1.5.5.7.3.8)
- Fecha de revocación: 28/12/2020

1.3.1.2.5 AC Firmaprofesional - Secure Web 2022

- CN = AC Firmaprofesional - Secure Web 2022
- Hash SHA1: 8b16eaed554db72788e54e9de5aad8db940f0d88
- Hash SHA256: C068D776784255772BBC6AE9F70A536A410AD688A50DDEAFBF66BCC5254796F6

- Válido desde el 4 de marzo de 2022 a 3 de marzo de 2025
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)

1.3.1.2.6 FIRMAPROFESIONAL ICA A01 QWAC 2022

- CN = FIRMAPROFESIONAL ICA A01 QWAC 2022
- Hash SHA1: 4A:B0:FF:8E:02:4B:CF:5D:97:69:CD:20:8B:72:51:61:85:AB:7E:EB
- Hash SHA256: CC:1B:9F:9E:43:70:FB:68:14:1D:28:A1:15:EA:A8:63:F8:EA:DB:7A:04:E2:BD:23:B3:C6:2F:9D:9F:17:C2:63
- Válido desde el 19 de julio de 2022 hasta el 18 de julio de 2027
- Tipo de Clave: SHA384 WITH ECDSA
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)

1.3.1.2.7 AC Firmaprofesional - Timestamp 2021

- CN = AC Firmaprofesional – Timestamp 2021
- Hash SHA1: 942a7aac5d23d4ecb317b919e2f4861cc1d605c9
- Hash SHA256: 75B14D4D63806F30F538060F2EB65C1365BFC0CD7F3ECDC6C0070218B6E46759
- Válido desde el 13 de abril de 2021 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 4096 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Impresión de fecha (1.3.6.1.5.5.7.3.8)

1.3.1.2.8 FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022

La Autoridad de Certificación Subordinada "FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022" emitirá certificados digitales para servicios de sellos de tiempo **cualificados**.

- CN = FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022
- Hash SHA1: 7A:5A:F7:61:64:EB:75:71:07:DA:93:FA:31:89:80:89:14:E4:1C:12
- Hash SHA256: 1F:3F:44:97:DF:9B:AC:9D:72:F9:99:75:B3:7D:ED:7D:5D:B9:30:05:B1:BF:80:E0:71:02:76:6F:3A:E4:05:B9
- Válido desde el 19 de julio de 2022 hasta el 31 de marzo de 2047
- Tipo de Clave: SHA384 WITH ECDSA
- Restricciones técnicas (extendedKeyUsage):
  - Time Stamping (1.3.6.1.5.5.7.3.8)

1.3.1.2.9 FIRMAPROFESIONAL CA ROOT-A WEB (CROSS)

Finalmente, se ha procedido a emitir una SubCA cruzada emitida desde la CA "Autoridad de Certificacion Firmaprofesional CIF A62634068"

- CN = FIRMAPROFESIONAL CA ROOT-A WEB
- Hash SHA1: AA:62:0B:07:97:A2:95:1E:E1:4C:12:4A:C0:F3:F4:73:4E:B7:20:8D
- Hash SHA256: FF:D0:08:5C:6C:35:69:F8:D4:12:BC:D8:E6:D1:B8:AC:F0:92:9A:41:F4:FD:35:94:F8:C0:F4:B6:D5:25:38:30
- Válido desde el 19 de julio de 2022 hasta el 5 de mayo de 2036
- Tipo de Clave: SHA256WITHRSA

1.3.1.2.10 AC Firmaprofesional - Secure Web 2024

- CN = AC Firmaprofesional - Secure Web 2024
- Hash SHA1: 88:43:C4:77:65:65:65:8D:EB:4D:4E:0A:F1:3C:15:C2:61:EF:5C:B0
- Hash SHA256: C3:F5:32:65:37:DB:64:77:C4:D7:BF:83:0F:F5:B4:01:A7:AD:B2:97:07:70:2A:DD:98:E6:24:61:F9:EE:67:C7
- Válido desde el 14 de febrero de 2024 a 13 de febrero de 2027

- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)

1.3.1.3 Autoridades de Certificación Subordinadas para servicios No Cualificados

Las Autoridades de Certificación Subordinadas para servicios no cualificados emiten certificados no cualificados. No están reconocidas en ninguna plataforma ni están reguladas por ningún organismo.

Firmaprofesional garantiza el mismo nivel de seguridad técnica a estos certificados que a los certificados públicos, ya que están operados desde la misma infraestructura y desde las mismas instalaciones.

1.3.1.3.1 AC Firmaprofesional - CFEA

La Autoridad de Certificación Subordinada "AC Firmaprofesional - CFEA" emite certificados digitales para servicios de firma electrónica, no cualificados.

Se dispone de cuatro versiones de este certificado, con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y dos con el algoritmo SHA2. Las versiones SHA2 están restringidas técnicamente mediante el uso de la extensión Extended Key Usage (EKU – extKeyUsage) según lo establecido en los Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates y Mozilla CA Certificate Inclusion Policy vigentes en el momento de entrada en vigor de la presente CPS.

- CN = AC Firmaprofesional - CFEA
- Hash SHA1: 6B66 7859 C1D8 C0F6 2F20 5B21 53D3 255C 7E16 CE0B
- Hash SHA256: 945853E4DF60E00B7A70294C34E8CD5F436B76F7DF5CA5BD5D822B72445692E6
- Válido desde el 20 de febrero de 2013 hasta el 31 de Diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA1
- Fecha de revocación: 16 de noviembre de 2018

- CN = AC Firmaprofesional - CFEA
- Hash SHA1: 3a 8f 3b b1 90 75 00 4a 29 cd 60 85 f3 49 2e 10 da b1 b7 b2
- Hash SHA256: 626403E07A393E707C88A470450491704B122B64D118323917DD4D41FC063C38
- Válido desde el 29 de julio de 2015 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Correo seguro (1.3.6.1.5.5.7.3.4)
    - Firma de OCSP (1.3.6.1.5.5.7.3.9)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
- Fecha de revocación: 16 de noviembre de 2018

- CN = AC Firmaprofesional - CFEA
- Hash SHA1: A2F7 8768 6F62 5F66 0679 AAF1 C861 3CA3 841B 9087
- Hash SHA256: E3C5244D15F8E0B034F500903B7DA11C57C1656175B86608C7FCDC561D081BF6
- Válido desde el 18 de junio de 2018 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits - SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Firma de OCSP (1.3.6.1.5.5.7.3.9)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

- Fecha de revocación: 6/08/2020

- CN = AC Firmaprofesional - CFEA
- Hash SHA1: 3cc6e9296172146c9a6cd6ce650e48e95e49a281
- Hash SHA256: 70E08EFCB3B574F562AB772B2BDCFF4E42D7C0A5FD457F1F9BB33346B522F294
- Válido desde el 9 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits - SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)
- Fecha de revocación: 11/11/2020

Se dispone de una quinta versión, con nuevas claves y nuevo campo CN:

- CN = AC Firmaprofesional - CFEA 2020
- Hash SHA1: 63957dbde8b5fa714ad34c0dd49bc141c604833f
- Hash SHA256: 3F4E45A8508BF83137F966AC961EF45AF573F25AA14D83C2A7F23B80A831C93C
- Válido desde el 30 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits - SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

1.3.1.3.2 AC Firmaprofesional – OTC

La Autoridad de Certificación Subordinada "AC Firmaprofesional – OTC" (OTC: one-time certificate) emite certificados digitales no cualificados, para servicios de firma electrónica. Estos certificados tendrán una vigencia muy corta y estarán limitados para la firma de un único documento.Se dispone de cuatro versiones de este certificado, con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y dos con el algoritmo SHA2.

Las versiones SHA2 están restringida técnicamente mediante el uso de la extensión Extended Key Usage (EKU – extKeyUsage) según lo establecido en los Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates y Mozilla CA Certificate Inclusion Policy en el momento de entrada en vigor de la presente CPS.

- CN = AC Firmaprofesional - OTC
- Hash SHA1: 1302 2ECD E763 0FB9 A14A 403E 74B0 FA3F A2A7 BCDA
- Hash SHA256: C9F3BB204DF689CA569157FB737E9E8B33905811577BDFF8FC376701D627581C
- Válido desde el 20 de febrero de 2013 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA1
- Fecha de revocación: 16 de noviembre de 2018

- CN = AC Firmaprofesional - OTC
- Hash SHA1: 6E13 B51C 6D54 0888 B8EC C236 79E9 1D99 AFF6 010D
- Hash SHA256: 831078F7E21FA71FE24F91D718E4A57329EFE6F4871B126115D5D273BFAD9F76
- Válido desde el 29 de julio de 2015 hasta el 31 de diciembre de 2030
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Correo seguro (1.3.6.1.5.5.7.3.4)
  - Firma de OCSP (1.3.6.1.5.5.7.3.9)
  - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
- Fecha de revocación: 16 de noviembre de 2018

- CN = AC Firmaprofesional - OTC

- Hash SHA1: 72DD 9D6D 7AE3 246C 6B9F 805F B2F6 216E 283C 4CE2
- Hash SHA256: 22B6EBDEE9B0A6DA5C9FACED27BF9DCE09803C2AFC11F76B5C0BCF47B7F7D560
- Válido desde el 18 de junio de 2018 hasta el 31 de diciembre de 2030

- Tipo de Clave: RSA 2048 bits - SHA256

- Restricciones técnicas (extendedKeyUsage):

    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)

    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)

    - Firma de OCSP (1.3.6.1.5.5.7.3.9)

    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

- Fecha de revocación: 6/08/2020

- CN = AC Firmaprofesional - OTC

- Hash SHA1: 62888877f290566b657d6e94e76be12e0ac66731
- Hash SHA256: 3774EC2D45F77668ED038F5256D339811D0915B8501D403FE2CF50ED753451E5

- Válido desde el 9 de julio de 2020 hasta el 31 de diciembre de 2030

- Tipo de Clave: RSA 2048 bits - SHA256

- Restricciones técnicas (extendedKeyUsage):

    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

- Fecha de revocación: 11/11/2020

Se dispone de una quinta versión, con nuevas claves y nuevo campo CN:

- CN = AC Firmaprofesional - OTC 2020

- Hash SHA1: 32adc15e7b31648da5fe3d0009e2a107cfe08b91
- Hash SHA256: 2E60F867E8887CE218059E85403F3613D28DA9EF658874D0C6F9FF25F2DDB6E5
- Válido desde el 30 de julio de 2020 hasta el 31 de diciembre de 2030

- Tipo de Clave: RSA 2048 bits - SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
    - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

1.3.1.3.3 FIRMAPROFESIONAL ICA A02 NO QWAC 2022

La Autoridad de Certificación Subordinada "FIRMAPROFESIONAL ICA A02 NO QWAC 2022" emitirá certificados digitales **no cualificados** de autenticación web.

- CN = FIRMAPROFESIONAL ICA A02 NO QWAC 2022
- Hash SHA1: 8C:D9:94:17:8E:3E:01:7C:62:F2:C5:20:CD:D3:DD:1A:8D:AF:28:F7
- Hash SHA256: 22:FD:54:F9:33:B1:7F:45:89:42:C3:45:E3:AE:62:5E:40:5C:E4:0B:19:1B:31:6B:88:7C:A3:D0:2C:CA:C3:B1
- Válido desde el 19 de julio de 2022 hasta el 18 de julio de 2027
- Tipo de Clave: SHA384 WITH ECDSA
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)

1.3.1.3.4 FIRMAPROFESIONAL ICA B03 NOQ 2022

La Autoridad de Certificación Subordinada "FIRMAPROFESIONAL ICA B03 NOQ 2022" emite certificados digitales para servicios de firma electrónica no cualificados.

- CN = FIRMAPROFESIONAL ICA B03 NOQ 2022
- Hash SHA1: 1D:FD:29:48:E6:7C:3E:94:9A:3E:E9:AC:D7:6F:2D:59:50:EA:0F:D6
- Hash SHA256: 4A:F8:B8:87:C3:EB:ED:C0:8B:FC:49:41:B2:BC:B6:FF:3B:62:92:F2:1E:A0:BA:6A:C6:C3:19:48:C3:83:CF:69
- Válido desde el 16 de junio de 2022 hasta el 31 de marzo de 2047
- Tipo de Clave: SHA384 WITH ECDSA
- Restricciones técnicas (extendedKeyUsage):

- Autenticación del cliente (1.3.6.1.5.5.7.3.2)
- Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
- Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

1.3.1.3.5 FIRMAPROFESIONAL ICA B04 NOQ TSU 2022

La Autoridad de Certificación Subordinada "FIRMAPROFESIONAL ICA B04 NOQ TSU 2022" emite certificados digitales para servicios de sellos de tiempo no cualificados.

- CN = FIRMAPROFESIONAL ICA B04 NOQ TSU 2022
- Hash SHA1: C1DB45C0913CFAE1D8F27B388E6CB3A933BB3A8C
- Hash SHA256:
  CD:65:B8:1A:AC:D1:17:0F:69:C6:60:14:32:27:04:9F:BF:15:17:19:E6:90:50:95:B9:5F:53:F5:3C:6D:13:4B
- Válido desde el 16 de junio de 2022 hasta el 31 de marzo de 2047
- Tipo de Clave: SHA384 WITH ECDSA
- Restricciones técnicas (extendedKeyUsage):
  - Time Stamping (1.3.6.1.5.5.7.3.8)

1.3.1.3.6 FIRMAPROFESIONAL ICA B05 NOQ OTC 2022

La Autoridad de Certificación Subordinada "FIRMAPROFESIONAL ICA B05 NOQ OTC 2022" (OTC: one-time certificate) emite certificados digitales no cualificados, para servicios de firma electrónica. Estos certificados tendrán una vigencia muy corta y estarán limitados para la firma de un único documento.

- CN = FIRMAPROFESIONAL ICA B05 NOQ OTC 2022

- Hash SHA1: CB:14:D0:72:15:52:F9:63:A4:9E:1B:DC:4C:F6:91:36:AB:98:FA:DF
- Hash SHA256:
  AF:76:9E:E4:98:EE:4B:20:B9:E5:7B:43:FE:6C:73:BD:D6:84:C5:32:2C:3E:5A:19:36:39:55:06:28:FD:7C:79
- Válido desde el 16 de junio de 2022 hasta el 31 de marzo de 2047
- Tipo de Clave: SHA384 WITH ECDSA

- Restricciones técnicas (extendedKeyUsage):

  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
  - Adobe Authentic Documents Trust (1.2.840.113583.1.1.5)

1.3.1.4 Autoridades de Certificación Subordinadas de otros PSC

Bajo la Jerarquía de Certificación de Firmaprofesional residen varias CAs Subordinadas emitidas a nombre de otras entidades. Estas otras entidades se deberán constituir como Prestadores de Servicios de Confianza y definir su propia Declaración de Prácticas de Certificación (CPS). Firmaprofesional garantiza el mismo nivel de seguridad técnica a estos certificados que a los certificados públicos, ya que están operados desde la misma infraestructura y desde las mismas instalaciones.

Actualmente la Jerarquía de Certificación de Firmaprofesional acoge a las CAs de otros 3 Prestadores de Servicios de Confianza.

1.3.1.4.1 SIGNE Autoridad de Certificacion

SIGNE S.A. (CIF-A11029279) es una empresa española cuya actividad principal es la edición e impresión de documentos de seguridad para empresas públicas y privadas.

Se dispone de tres versiones de este certificado, todas ellas con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y las otras con el algoritmo SHA2. Éstas dos últimas está restringida técnicamente mediante el uso de la extensión Extended Key Usage (EKU – extKeyUsage) según lo establecido en los Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates y Mozilla CA Certificate Inclusion Policy vigentes en el momento de entrada en vigor de la presente CPS.

- CN = SIGNE Autoridad de Certificacion
- Hash SHA1: D730 47F2 CCE5 64EF B0BC 8568 93EA 19D7 7469 398C
- Hash SHA256: 0431D736C77697A0310103C6F890BC41C3A3BB81128ADE8D3C3461B4028D4413
- Válido desde el 21 de julio de 2.010 hasta el 21 de julio de 2.022
- Tipo de clave: RSA 2048 bits – SHA1
- CPS: https://www.signe.es/signe-ac/dpc
- Fecha de revocación: 22/10/2019https://www.signe.es/signe-ac/dpc

- CN = SIGNE Autoridad de Certificacion
- Hash SHA1: E6B5 2B5D 52E5 CDE9 862A C1DE 668E C953 AD36 59BD
- Hash SHA256: 1CB470728CF56F302003BB0E4EB062414FA11D4F97E3F061170C96C88071D711
- Válido desde el 29 de julio de 2015 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Correo seguro (1.3.6.1.5.5.7.3.4)
  - Firma de OCSP (1.3.6.1.5.5.7.3.9)
  - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
- CPS: https://www.signe.es/signe-ac/dpc
- Fecha de revocación: 28/12/2020https://www.signe.es/signe-ac/dpc

- CN = SIGNE Autoridad de Certificacion
- Hash SHA1: f3b9903d00e5172ca359c020ec0c2a1f7307dbeb
- Hash SHA256: C42CE022D0A3457B6BD6978711CE7BC74385C4B34E11EBC8BAEE8B1D1B832799
- Válido desde el 9 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Correo seguro (1.3.6.1.5.5.7.3.4)
- CPS: https://www.signe.es/signe-ac/dpc
- Fecha de revocación: 28/12/2020

Se dispone de una cuarta versión, con nuevas claves y nuevo campo CN:

- CN = SIGNE Autoridad de Certificacion - 2020
- Hash SHA1: d2b38ebe17a8b8956810ece820a5718811378653

- Hash SHA256: B8DF384F1FCD6ECB3F4D7DD6380E54D354C61256560A599D80453247D93AF5EA
- Válido desde el 30 de julio de 2020 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Correo seguro (1.3.6.1.5.5.7.3.4)
- CPS: https://www.signe.es/signe-ac/dpc

1.3.1.4.2 SEU Autoridad de Certificacion

SEU (Servicios Electrónicos Universitarios) es una empresa colombiana enfocada al servicio de instituciones universitarias de Colombia en el ámbito de la administración electrónica.

Se dispone de dos versiones de este certificado, ambas con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y otra con el algoritmo SHA2. Ésta segunda está restringida técnicamente mediante el uso de la extensión Extended Key Usage (EKU – extKeyUsage), según lo establecido en los Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates y Mozilla CA Certificate Inclusion Policy vigentes en el momento de entrada en vigor de la presente CPS.

Ambos certificados han sido revocados debido al cese de las operaciones de este Prestador de Servicios de Confianza.

- CN = SEU Autoridad de Certificacion
- Hash SHA1: 432C 2A08 ED3E 4ACB 87E8 4704 DCFD 9C3B D84D 18B7
- Hash SHA256: B89F5810BB6B8FA138DEC358159AC01363883F0B9870AEA51922A7EA0EC6DD13
- Válido desde el 20 de febrero de 2013 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA1
- CPS: http://www.seu.com.co/dpc
- Fecha de revocación: 6 de julio de 2017 http://www.seu.com.co/dpc

- CN = SEU Autoridad de Certificacion
- Hash SHA1: A9E5 5245 74A8 EC1F D316 1854 C913 4C47 97DE 7B09
- Válido desde el 29 de julio de 2015 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
    - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
    - Correo seguro (1.3.6.1.5.5.7.3.4)
    - Firma de OCSP (1.3.6.1.5.5.7.3.9)
    - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
- CPS: http://www.seu.com.co/dpc
- Fecha de revocación: 23/06/2017
  http://www.seu.com.co/dpc

1.3.1.4.4 Santander Digital Signature

Banco Santander ofrece sus servicios de certificación electrónica en el ámbito universitario mediante la emisión de la Tarjeta Universitaria Inteligente (TUI).

Se dispone de dos versiones de este certificado, ambas con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y otra con el algoritmo SHA2. Ésta segunda está restringida técnicamente mediante el uso de la extensión Extended Key Usage (EKU – extKeyUsage) según lo establecido en los Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates y Mozilla CA Certificate Inclusion Policy vigentes en el momento de entrada en vigor de la presente CPS.

Ambos certificados han sido revocados debido al cese de las operaciones de este Prestador de Servicios de Confianza.

- CN = Santander Digital Signature
- Hash SHA1: CF4E 801B 2774 B820 6A62 6371 AE32 37B7 C1D4 3F4E
- Hash SHA256: CBC689C87A63FA7323A7607CC7C457B3B450572BEFA47470B61C35BF079B600B
- Hash MD5: 1CD9 FA19 8BEE A19E 8658 7D90 58BE 3E88
- Válido desde el 16 de mayo de 2012 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA1
- CPS: http://www.tuisantander.com/cps
- Fecha de revocación: 18 de junio de 2018

http://www.tuisantander.com/cps

- CN = Santander Digital Signature
- Hash SHA1: B00C 0003 4B72 3F4D 9537 353C 8293 A945 514D AB2D
- Hash SHA256: D039EEFF71088CC0F16A05A8FF3C61610E141D1E850AC7E11F7713EEE88CB951
- Válido desde el 29 de julio de 2015 hasta el 31 de diciembre de 2030
- Tipo de clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
  - Correo seguro (1.3.6.1.5.5.7.3.4)
  - Firma de OCSP (1.3.6.1.5.5.7.3.9)
  - Inicio de sesión de tarjeta inteligente (1.3.6.1.4.1.311.20.2.2)
- CPS: http://www.tuisantander.com/cps
- Fecha de revocación: 18 de junio de 2018

1.3.1.5 Autoridades de Certificación Caducadas

1.3.1.5.1 Autoridad de Certificación Raíz

El Certificado Raíz original de Firmaprofesional caducó el 24 de Octubre 2013. Este certificado fue sustituido por un nuevo Certificado Raíz con otras claves.

- CN = Autoridad de Certificacion Firmaprofesional CIF A62634068
- Hash SHA1: A962 8F4B 98A9 1B48 35BA D2C1 4632 86BB 6664 6A8C
- Hash SHA256: C1CF0B52096435E3F1B71DAAEC455A2311C8404F5583A9E213C69D857D943305
- Hash MD5: 1192 7940 3CB1 8340 E5AB 664A 6792 80DF
- Válido desde el 24 de octubre de 2001 al 24 de Octubre de 2013
- Longitud de clave RSA 2048 bits

1.3.1.5.2 AC Firmaprofesional - CA1

El certificado de la Autoridad de Certificación Subordinada "AC Firmaprofesional - CA1" caducó en 2013 y también fue renovado.

En este caso se renovó manteniendo las claves y el nombre. Este modelo de certificación con claves compartidas recibe el nombre de "Certificación Cruzada". Gracias a ello los certificados de usuarios finales emitidos podrían validarse tanto con la jerarquía basada en la CA que caduca en 2013 como con la jerarquía basada en la CA que caduca en 2030.

Los datos identificación del Certificado de CA Subordinada de Firmaprofesional caducado en 2013:

- CN = AC Firmaprofesional - CA1
- Hash SHA1: 037C F211 8F13 EAA6 121E B035 6F9B 601C 9295 338E
- Hash SHA256: 65BA8FC0CE3C434164DC40815A6CA6FB44C7272046FCD303A29DA8F41CA2075D
- Hash MD5: 35D8 35EC AF1C AF08 7DD5 8727 8AB2 0B19
- Válido desde el 27 de marzo 2003 al 26 de marzo de 2013
- Longitud de clave RSA 2048 bits

1.3.1.5.3 AC Firmaprofesional - AAPP

La Autoridad de Certificación Subordinada "AC Firmaprofesional - AAPP" emite certificados digitales a Corporaciones Públicas, conforme la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Se dispone de dos versiones de este certificado, ambos con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y otra con el algoritmo SHA2:

- CN = AC Firmaprofesional - AAPP
- Hash SHA1: E678 37DC 4C75 EA77 458C 14C3 6B5C 0DA6 512C 6FC0
- Hash SHA256: 83F6F017C2536D7454B7B9848674F3640129CF555DD07D83D362A17C81B7525F
- Válido desde el 7 de julio 2010 hasta el 7 de julio de 2022
- Tipo de Clave: RSA 2048 bits – SHA-1

- CN = AC Firmaprofesional - AAPP
- Hash SHA1: 3E74 9302 FEB9 6904 AFEA 06FE 220A CBF4 08CF EDFA
- Hash SHA256: 6365B25E9299B5F382EB0066850629088EBCD9BCB398F28622107603C3C1C27E
- Válido desde el 25 de octubre 2016 hasta el 7 de julio de 2022
- Tipo de Clave: RSA 2048 bits – SHA-2

1.3.1.5.4 AC Firmaprofesional - Secure Web 2020

- CN = AC Firmaprofesional - Secure Web 2020
- Hash SHA1: 99d9b30876702971510942ec64d456e1aa7e4951
- Hash SHA256: 933B80F7B97255DF5CF1D95A123E901722DDB30B481AF3AA83548201119ED303
- Válido desde el 30 de julio de 2020 hasta el 30 de julio de 2023
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)
- Fecha de revocación: 03/11/2022

1.3.1.5.5 AC Firmaprofesional - Secure Web 2021

- CN = AC Firmaprofesional - Secure Web 2021
- Hash SHA1: 8e7d98607ecfc6926ed4ed48edaf018fc3d04230
- Hash SHA256: 59228535D114E8D29F9B92D422518BC63DDCB57097428D8CC98777D907C6EEFE
- Válido desde el 5 de marzo de 2021 a 4 de marzo de 2024
- Tipo de Clave: RSA 2048 bits – SHA256
- Restricciones técnicas (extendedKeyUsage):
  - Autenticación del servidor (1.3.6.1.5.5.7.3.1)
  - Autenticación del cliente (1.3.6.1.5.5.7.3.2)

1.3.2 Autoridad de Registro (RA)

Una Autoridad de Registro (en inglés RA o Registration Authority) de Firmaprofesional, es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado
- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor.

Podrán actuar como RA de Firmaprofesional:

- Cualquier Corporación que sea cliente de Firmaprofesional, para la emisión de certificados a nombre de la corporación o a miembros de la corporación.
- Cualquier entidad de confianza que llegue a un acuerdo con Firmaprofesional para actuar como intermediario en nombre de Firmaprofesional.
- La propia Firmaprofesional directamente.

Firmaprofesional formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como RA de Firmaprofesional.

La entidad que actúe como RA de Firmaprofesional podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema informático de emisión de certificados de Firmaprofesional en nombre de la RA.

1.3.2.1 Entidad Solicitante

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del suscriptor y en la solicitud y entrega de certificados, la RA podrá delegar

estas funciones a una entidad de confianza. Dicha entidad deberá tener una especial vinculación con la RA y una relación de proximidad con los suscriptores de los certificados que justifique la delegación.

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. Por lo tanto, será el propietario del certificado.

En general, el suscriptor de un certificado de Firmaprofesional será un Colegio profesional/Administración Pública, organismo o entidad de derecho público/empresa, la identidad de la cual aparecerá en el propio certificado. En este caso el suscriptor podrá actuar como RA, gestionando la emisión de los certificados a nombre de la corporación o a miembros de la corporación.

Cuando la venta del certificado se realiza directamente por Firmaprofesional a una persona física, la figura del suscriptor y del firmante coinciden en dicha persona física.

1.3.3.1 Solicitante

Solicitante es la persona física que, en nombre propio o en representación de un tercero, solicita la emisión de un certificado a Firmaprofesional.

Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

1.3.3.2 Firmante

El Firmante se trata de la persona física que crea una firma electrónica actuando en su propio nombre y derecho, o bien, como sujeto que pertenece a un subscriptor corporativo (Colegio profesional, Administración Pública, organismo o entidad de derecho público, empresa).

Corresponde al firmante la custodia de los datos de creación de firma asociados a cada uno de los certificados electrónicos.

1.3.4 Tercero que confía en los certificados

Se entiende como tercero que confía en los certificados (en inglés, relying party) a toda persona u organización que voluntariamente confía en un certificado emitido por Firmaprofesional.

Los certificados cualificados emitidos por Firmaprofesional tienen carácter universal y están aceptados por la mayoría de los organismos públicos del Estado español, como Ministerios, CCAA, Diputaciones o Ayuntamientos. Firmaprofesional tratará de establecer acuerdos con el mayor número de entidades posible para el reconocimiento de sus certificados cualificados.

Los Certificados Raíz de Firmaprofesional están reconocidos por los principales fabricantes de software como Microsoft, Fundación Mozilla o Apple.

Las obligaciones y responsabilidades de Firmaprofesional con terceros que voluntariamente confíen en los certificados se limitarán a las recogidas en esta CPS, en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en el Reglamento UE 910/2014.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

1.3.5 Otros participantes

Sin estipulación.

1.4 Uso de los Certificados

1.4.1 Uso adecuado de los certificados

El uso y las limitaciones de los certificados se recogerán en la política de cada uno de los certificados que se emiten por Firmaprofesional.

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 Declaración de Prácticas de Certificación y en su correspondiente Política de Certificación.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Los certificados de usuario final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

Firmaprofesional por regla general no almacena copias de las claves privadas del suscriptor de certificados, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor.

Cuando Firmaprofesional custodia la clave privada de los suscriptores éstas están custodiadas por un dispositivo criptográfico hardware certificado EAL4+, garantizando que la misma nunca está en claro fuera del dispositivo criptográfico y que la activación y uso de dicha clave sólo puede ser realizada por el firmante.

El Suscriptor que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, Firmaprofesional tenga responsabilidad alguna por pérdida de información derivada de la pérdida de las claves de cifrado. Por ello, Firmaprofesional no recomienda el uso de los certificados digitales para el cifrado de la información.

1.4.2.1 Notificación de usos no autorizados, compromiso de clave, quejas o sugerencias

En caso de detectar un uso no autorizado de los certificados, compromiso de clave según el apartado correspondiente de esta CPS 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", un "compromiso de clave", 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 las políticas

1.5.1 Organización responsable

El Departamento Técnico de Firmaprofesional es responsable de la administración de esta CPS, de las Políticas de Certificación y de los textos de divulgación-PDS.

1.5.2 Persona de contacto

Organización responsable:	Firmaprofesional, S.A.
Persona de contacto:	Responsable de Cumplimiento de Firmaprofesional
E-mail:	compliance@firmaprofesional.com
Teléfono:	+34 93 477 42 45
Dirección:	Firmaprofesional, S.A. Passeig de Gràcia 50, 2-1 08007 Barcelona
Quejas, sugerencias y comunicación de, sospecha de compromiso de clave privada, uso indebido de certificados u otros tipos de fraude, compromiso, uso indebido, conducta inapropiada o cualquier otro asunto relacionado con los certificados	soporte@firmaprofesional.com

1.5.3 Frecuencia de revisión

La CPS y las distintas CP y PDS, serán revisadas y actualizadas anualmente.

Asimismo, la Política de Seguridad de Firmaprofesional se revisará a intervalos planificados, como mínimo anualmente y, en todo caso si se producen cambios significativos en la organización con el objetivo de mantener la idoneidad, adecuación y eficacia de la misma.

1.5.4 Procedimiento de aprobación

La publicación de las revisiones de esta CPS y de las Políticas de Certificación y Textos de Divulgación-PDS de cada tipo de certificado deberá ser aprobada por la Dirección General de Firmaprofesional, después de comprobar el cumplimiento de los requisitos expresados en ella.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

- **Prestador de Servicios de Certificación**: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **Prestador de Servicios de Confianza**: persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza;
- **Certificado Electrónico**: un documento firmado electrónicamente por un prestador de servicios de confianza que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
- **Certificado Cualificado**: Certificado expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el Anexo I del Reglamento UE 910/2014 (eIDAS) y que cumple los requisitos establecidos en el artículo 7 de la Ley 6/2020 (LSEC) en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de confianza que presten, de conformidad con el Título III de la mencionada Ley 6/2020 LSEC .
- **Clave Pública y Clave Privada**: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

- **Conformity Assessment Body**: organismos acreditados por los estados miembro para poder emitir informes de conformidad según lo requerido por eIDAS.

- **Datos de Creación de Firma (Clave Privada)**: son datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

- **Datos de Verificación de Firma (Clave Pública)**: son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

- **Dispositivo Cualificado de Creación de Firma / de Sello electrónico (DCCF)**: Dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014 DEL PARLAMENTO EUROPEO 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.

- **Firma Electrónica**: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

- **Firma Electrónica Avanzada**: es aquella firma electrónica que permite establecer la identidad personal del firmante respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al firmante, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

- **Firma Electrónica Cualificada**: es aquella firma electrónica avanzada basada en un certificado cualificado y generada mediante un dispositivo cualificado de creación de firma.

- **Función Hash**: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

- **Listas de Certificados Revocados (CRL)**: lista donde figuran las relaciones de certificados revocados o suspendidos.

- **Módulo Criptográfico Hardware (HSM)**: módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

- **Sello de Tiempo Electrónico**: es un tipo especial de firma electrónica emitida por un tercero de confianza que permite garantizar la integridad de un documento en una fecha y hora determinadas.

- **Sello Cualificado de Tiempo Electrónico**: es un sello de tiempo electrónico que cumple los requisitos establecidos en artículo 42 del Reglamento UE 910/2014 (eIDAS).

- **Autoridad de Sellado de Tiempo (TSA)**: Entidad de confianza que emite sellos de tiempo.

- **Autoridad de Validación (VA)**: Entidad de confianza que proporciona información sobre la validez de los certificados digitales y de las firmas electrónicas.

1.6.2 Acrónimos

CA:	Autoridad de Certificación (Certification Authority)
CA Sub:	Autoridad de Certificación Subordinada
CAB	Conformity Assessment Body
CP:	Política de Certificación (Certificate Policy)
CPS:	Declaración de Prácticas de Certificación (Certification Practices Statement)
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol
OID:	Identificador de objeto único (Object identifier)
PDS	Texto de Divulgación (PKI Disclosure Statement)
PKI:	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC:	Prestador de Servicios de Confianza
RA:	Autoridad de Registro (Registration Authority)
TSA:	Autoridad de sellado de tiempo (Time Stamp Authority)
VA	Autoridad de validación (Validation Authority)

Estándares y Organismos de estandarización

CEN:	Comité Europeo de Normalización
CWA:	CEN Workshop Agreement
ETSI:	European Telecommunications Standard Institute

FIPS:	Federal Information Processing Standard
IETF:	Internet Engineering Task Force
PKIX:	Grupo de trabajo del IETF sobre PKI
PKCS:	Public Key Cryptography Standards
RFC:	Request For Comments

2 Repositorios y publicación de información

2.1 Repositorios

Acceso	Descripción	URL
Público	CPS, Políticas de Certificación y PDS	http://www.firmaprofesional.com/cpshttp://www.firmaprofesional.com/cps
Público	CA Raíz	http://crl.firmaprofesional.com/caroot.crthttp://crl.firmaprofesional.com/caroot.crt
Público	CRL de CA Raíz	http://crl.firmaprofesional.com/fproot.crlhttp://crl.firmaprofesional.com/fproot.crl
Público	FIRMAPROFESIONAL CA ROOT-A WEB	http://crl.firmaprofesional.com/caroot-a_web.crt
Público	CRL de FIRMAPROFESIONAL CA ROOT-A WEB	http://crl.firmaprofesional.com/caroot-a_web.crl
Público	FIRMAPROFESIONAL CA ROOT-B GP	http://crl.firmaprofesional.com/caroot-b_gp.crt
Público	CRL de FIRMAPROFESIONAL CA ROOT-B GP	http://crl.firmaprofesional.com/caroot-b_gp.crl
Público	FIRMAPROFESIONAL CA ROOT-C LATAM	http://crl.firmaprofesional.com/caroot-c_latam.crl
Público	CRL de FIRMAPROFESIONAL CA ROOT-C LATAM	http://crl.firmaprofesional.com/caroot-c_latam.crt
Público	CA Subordinada CA1	http://crl.firmaprofesional.com/ca1.crthttp://crl.firmaprofesional.com/ca1.crt
Público	CRL de CA Sub CA1	http://crl.firmaprofesional.com/firmaprofesional1.crlhttp://crl.firmaprofesional.com/firmaprofesional1.crl
Público	CA Subordinada AAPP	http://crl.firmaprofesional.com/fpaapp.crthttp://crl.firmaprofesional.com/fpaapp.crt
Público	CRL de CA Sub AAPP	http://crl.firmaprofesional.com/fpaapp.crlhttp://crl.firmaprofesional.com/fpaapp.crl
Público	CA Subordinada CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crt http://crl.firmaprofesional.com/cualificados.crt
Público	CRL de CA Sub CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crlhttp://crl.firmaprofesional.com/cualificados.crl
Público	CA Sub INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crthttp://crl.firmaprofesional.com/infraestructura.crt
Público	CRL de CA Sub INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crlhttp://crl.firmaprofesional.com/infraestructura.crl

Público	CA Subordinada CFEA	http://crl.firmaprofesional.com/cfea.crthttp://crl.firmaprofesional.com/cfea.crt
Público	CRL de CA Sub CFEA	http://crl.firmaprofesional.com/cfea.crlhttp://crl.firmaprofesional.com/cfea.crl
Público	CA Subordinada CFEA	http://crl.firmaprofesional.com/otc.crthttp://crl.firmaprofesional.com/otc.crt
Público	CRL de CA Sub CFEA	http://crl.firmaprofesional.com/otc.crlhttp://crl.firmaprofesional.com/otc.crl
Público	Servicio de Revocación	http://www.firmaprofesional.comhttp://www.firmaprofesional.com/
Restringido	Servicio de Sellado de Tiempo (TSA)	http://servicios.firmaprofesional.com/tsahttp://servicios.firmaprofesional.com/tsa
Restringido	Servicio de Validación (OCSP)	http://servicios.firmaprofesional.com/ocsphttp://servicios.firmaprofesional.com/ocsp
Público	Servicio de Validación (OCSP)	http://ocsp.firmaprofesional.comhttp://ocsp.firmaprofesional.com/
Público	CA Subordinada Secure Web 2020	https://crl.firmaprofesional.com/secureweb2020.crt
Público	CRL de CA Subordinada Secure Web 2020	https://crl.firmaprofesional.com/secureweb2020.crl
Público	CA Subordinada Secure Web 2021	https://crl.firmaprofesional.com/secureweb2021.crt
Público	CRL de CA Subordinada Secure Web 2021	https://crl.firmaprofesional.com/secureweb2021.crl
Público	CA Subordinada Secure Web 2022	https://crl.firmaprofesional.com/secureweb2022.crt
Público	CRL de CA Subordinada Secure Web 2022	https://crl.firmaprofesional.com/secureweb2022.crl
Público	CA Subordinada Secure Web 2024	https://crl.firmaprofesional.com/secureweb2024.crt
Público	CRL de CA Subordinada Secure Web 2024	https://crl.firmaprofesional.com/secureweb2024.crl
Público	CA Subordinada CFEA 2020	https://crl.firmaprofesional.com/cfea2020.crt

Público	CRL de CA Subordinada CFEA 2020	https://crl.firmaprofesional.com/cfea.crl
Público	CA Subordinada OTC 2020	https://crl.firmaprofesional.com/otc2020.crt
Público	CRL de CA Subordinada OTC 2020	https://crl.firmaprofesional.com/otc2020.crl
Público	CA Subordinada FIRMAPROFESIONAL ICA A01 QWAC 2022	http://crl.firmaprofesional.com/caroot-a_web.crt
Público	CRL de CA FIRMAPROFESIONAL ICA A01 QWAC 2022	http://crl.firmaprofesional.com/caroot-a_web.crl
Público	CA Subordinada FIRMAPROFESIONAL ICA A02 NO QWAC 2022	http://crl.firmaprofesional.com/caroot-a_web.crt
Público	CRL de CA FIRMAPROFESIONAL ICA A02 NO QWAC 2022	http://crl.firmaprofesional.com/caroot-a_web.crl
Público	CA Subordinada FIRMAPROFESIONAL ICA B01 QUALIFIED 2022	https://crl.firmaprofesional.com/ica-b01-q.crt
Público	CRL de CA FIRMAPROFESIONAL ICA B01 QUALIFIED 2022	https://crl.firmaprofesional.com/ica-b01-q.crl
Público	CA Subordinada FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022	https://crl.firmaprofesional.com/ica-b02-qtsa.crt
Público	CRL Subordinada FIRMAPROFESIONAL ICA B02 QUALIFIED QTSA 2022	https://crl.firmaprofesional.com/ica-b02-qtsa.crl

Público	CA Subordinada FIRMAPROFESIONAL ICA B03 NOQ 2022	https://crl.firmaprofesional.com/ica-b03-noq.crt
Público	CRL de CA FIRMAPROFESIONAL ICA B03 NOQ 2022	https://crl.firmaprofesional.com/ica-b03-noq.crl
Público	CA Subordinada FIRMAPROFESIONAL ICA B04 NOQ TSU 2022	https://crl.firmaprofesional.com/ica-b04-noqtsu.crt
Público	CRL de CA FIRMAPROFESIONAL ICA B04 NOQ TSU 2022	https://crl.firmaprofesional.com/ica-b04-noqtsu.crl
Público	CA Subordinada FIRMAPROFESIONAL ICA B05 NOQ OTC 2022	https://crl.firmaprofesional.com/ica-b05-noqotc.crt
Público	CRL de CA FIRMAPROFESIONAL ICA B05 NOQ OTC 2022	https://crl.firmaprofesional.com/ica-b05-noqotc.crl

Los repositorios de Firmaprofesional están referenciados por la URL. Cualquier cambio en las URLs se notificará a todas las entidades que puedan verse afectadas.

Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso.

2.2 Publicación de información

2.2.1 Políticas y Prácticas de Certificación

La CPS actual, las Políticas de Certificación y los Textos de Divulgación-PDS de cada tipo de certificado estarán disponibles en formato electrónico en la Web de Firmaprofesional.

Firmaprofesional mantiene publicadas aquellas versiones anteriores mientras existan certificados vigentes que se hayan emitido de acuerdo con dichos documentos.

Las demás versiones anteriores serán retiradas de su consulta on-line, pero podrán ser solicitadas por los interesados en la dirección de contacto de Firmaprofesional.

2.2.2 Términos y condiciones

La relación contractual entre Firmaprofesional y los Suscriptores está basada en la firma de un Contrato de Prestación de Servicios de Confianza y la aceptación de la Declaración de Prácticas de Certificación y las CP y PDS que correspondan de Firmaprofesional publicadas en su web http://www.firmaprofesional.com/cps

2.2.3 Difusión de los certificados

El firmante (o el Suscriptor del certificado cuando sean diferentes personas) será el responsable de hacer llegar su certificado a todo aquel tercero que desee autenticar a un usuario o comprobar la validez de una firma. Este envío se realizará generalmente de manera automática, adjuntando el certificado a todo documento firmado electrónicamente.

2.3 Frecuencia de publicación

La CA Raíz emitirá una Lista de CAs Revocadas (ARL) como mínimo cada seis meses, o extraordinariamente, cuando se produzca la revocación de un certificado de autoridad.

Cada CA Subordinada emitirá una Lista de Certificados Revocados (CRL) diariamente, y de forma extraordinaria, cada vez que se suspenda o revoque un certificado.

Firmaprofesional publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación.

2.4 Control de acceso a los repositorios

La CPS, las Políticas de Certificación, las PDS (PKI disclosure statement), los certificados de CA y las listas de certificados revocados (CRL) se publicarán en repositorios de acceso público sin control de acceso.

Las auditorías requeridas por los BRs así como las certificaciones emitidas se publican en repositorios públicos.

Los servicios de validación por el protocolo OCSP serán servicios de acceso público y gratuito.

Los servicios de sellado de tiempo por el protocolo TSP serán servicios de acceso restringido y de pago.

3 Identificación y autenticación

3.1 Registro de Nombres

3.1.1 Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500. Adicionalmente, todos los nombres de los certificados cualificados son coherentes con lo dispuesto en el apartado 7.1. Perfil de los certificados.

3.1.2 Necesidad de que los nombres sean significativos

Los campos del DN referentes al Nombre y Apellidos se corresponderán 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.

Los nombres distintivos de los certificados deben tener sentido.

3.1.3 Uso de seudónimos

En general, los certificados no admiten el uso de seudónimo de firmante, excepto y únicamente en los certificados del tipo "empleado público con seudónimo".

3.1.4 Reglas para interpretar varios formatos de nombres

Firmaprofesional atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594, así como por la RFC 5280 y por los Requerimientos de CA/Browser-Forum (Baseline Requirements y EV Guidelines).

Los campos en los certificados vinculados con datos de la persona física o jurídica que consten en los registros oficiales deberán aparecer, exactos y conformes a dichas fuentes oficiales.

3.1.5 Unicidad de los nombres

El nombre distinguido (DN) de los certificados emitidos será único para cada suscriptor o firmante. El atributo de CIF o NIF se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

3.1.6 Reconocimiento, autenticación y papel de las marcas registradas

La CA no asume compromisos en la emisión de certificados respecto al uso por los suscriptores de una marca comercial. Firmaprofesional no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del suscriptor. Si un solicitante alega tener derecho sobre una marca que desee incorporar en un certificado, la CA buscará evidencias de la posesión de derecho sobre la marca solicitada antes de la emisión de los certificados, a través la consulta a registros oficiales o documentos expedidos por los mismos.

3.2 Validación inicial de la identidad

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".

La selección de las Fuentes de Verificación se hace en base a los siguientes criterios:

- Entidad generadora de datos: Se evalúa la rigurosidad de la entidad emisora de los datos, dando especial relevancia a las fuentes de verificación generadas por entidades gubernamentales, organismos oficiales con jurisdicción de la creación, existencia o reconocimiento legal de organizaciones o entidades privadas consideradas como fuentes de información calificadas como independientes, tanto nacionales como internacionales.
- Frecuencia de actualización de datos de la fuente: La fuente debe actualizarse al menos 1 vez al año.
- La relativa dificultad de falsificar o alterar los datos suministrados por dicha fuente.

3.2.1 Método de prueba de posesión de la clave privada

Cuando se expide un certificado en un dispositivo hardware, la clave privada se crea en el instante previo a la generación del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con la identidad del solicitante.

Cada RA es responsable de garantizar la entrega o el acceso al dispositivo al solicitante de forma segura.

En los otros casos, el método de prueba de la posesión de la clave privada por el suscriptor será la entrega de PKCS#10 o una prueba criptográfica equivalente u otro método aprobado por Firmaprofesional.

3.2.2 Autenticación de la identidad de una persona jurídica e identidad de dominio

La Autoridad de Registro deberá verificar los siguientes datos para poder autenticar la identidad de la organización:

- Los datos relativos a la denominación o razón social de la organización.
- Los datos relativos a la constitución, y personalidad jurídica del suscriptor.
- Los datos relativos a la extensión y vigencia de las facultades de representación del solicitante.
- Los datos relativos al código de identificación fiscal de la organización o código equivalente utilizado en el país a cuya legislación esté sujeto el suscriptor.

Firmaprofesional se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

3.2.2.1 Validación del dominio

Para validar que una entidad solicitante tiene control sobre el dominio (URL) que solicita incluir en un certificado de autenticación web se realizará según lo estipulado en la correspondiente política de certificados de autenticación de sitio web.

3.2.2.2 Validación del correo electrónico

En general, los firmantes son personas vinculadas con la Autoridad de Registro (por ejemplo, colegiados, miembros de asociaciones, etc.) En estos casos no es el firmante el que solicita una determinada dirección de correo electrónico para ser incluida en el certificado, sino que es la propia RA la que, consultando sus bases de datos, obtiene dicha dirección.

En los casos en los que el firmante no tenga vínculo alguno con la RA, el control de la dirección de correo se realiza mediante desafío y respuesta a la dirección solicitada.

3.2.3 Autenticación de la identidad de una persona física

La RA verificará la identidad de la persona física identificada en el certificado. Para ello, la persona física deberá personarse y presentar el Documento Nacional de Identidad, tarjeta de residencia, pasaporte u otro medio reconocido en derecho que le identifique.

Las evidencias acerca de la identidad de la persona física podrán ser proporcionadas por una persona subcontratada que haya verificado la identidad de dicha persona física siguiendo los requerimientos establecidos en este apartado.

Se podrá emplear el método de identificación remota por video identificación asistida y desasistida según dispone el artículo 7.2 de la Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza y conforme al artículo artículo 24.1.d) del Reglamento (UE) 910/2014 eIDAS, cumpliendo las condiciones y requisitos organizativos y técnicos establecidos por Orden Ministerial, y previa su evaluación por un organismo de evaluación de la conformidad.

En caso que el suscriptor reclame la modificación de los datos de identificación personales a registrar respecto de los del documento de identificación presentado, deberá presentar el correspondiente Certificado del Registro Civil consignando la variación.

En caso de que la RA sospeche que el solicitante, aparentemente, no está en plenitud de sus facultades, no tiene capacidad de comprender las condiciones relativas a la utilización del servicio, o que no podrá tener el control exclusivo sobre los datos de creación de firma por diferentes causas, como por ejemplo, que no será capaz de usar o descargarse el certificado o de memorizar o custodiar el PIN de activación de la firma, el operador podrá solicitar a iniciativa propia la siguiente documentación:

- Certificado del Registro civil sobre "Modificaciones judiciales de la capacidad de las personas" o la Resolución judicial de incapacidad total o parcial.

  Si la incapacidad es total, no se podrá emitir el certificado.

  Si la incapacidad es parcial, el Operador verificará en la sentencia que declara la incapacidad parcial, si entre los actos en los que el afectado carece de capacidad para autogobernarse, se le ha declarado incapaz para solicitar un certificado o realizar firmas electrónicas o de forma más genérica, para manifestar su consentimiento.

  Si en el certificado del registro NO aparece inscripción de incapacitación judicial, pero persistiera la sospecha en el momento de la solicitud, el operador de la RA podrá realizar preguntas básicas sobre los usos a realizar con el certificado y si la incoherencia de las respuestas es permanente y absoluta, de conformidad con el Título X del Código Civil, podrá poner en conocimiento del Ministerio Fiscal o de la autoridad judicial el hecho determinante que ha suscitado la negativa de registrar al solicitante, para que estas autoridades acuerden lo procedente. Se podrá emitir el certificado si NO existe incapacidad, o sospecha de la misma, para alguno de los actos descritos en el párrafo anterior. En caso contrario el operador deberá no emitir el certificado justificando dicha decisión.

La RA verificará, bien mediante la exhibición de documentación original suficiente, bien con sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado (nombre distinguido del certificado), debiendo guardar la documentación acreditativa de la validez de aquellos datos que no puede comprobar por medio de sus propias fuentes de datos.

Lo dispuesto en los párrafos anteriores podrá no ser exigible de conformidad con Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza, en los siguientes casos:

a. Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la RA en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en el párrafo primero y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b. Cuando para solicitar un certificado se utilice otro para cuya expedición se hubiera identificado al firmante en la forma prescrita en el párrafo primero y le conste a la RA que el período de tiempo transcurrido desde la identificación es menor de cinco años.

3.2.4 Información del suscriptor no verificada

Toda la información de los certificados SSL está verificada previamente a la emisión de los mismos contrastando con fuentes de información independientes.

3.2.5 Autenticación de la identidad de la RA y de operadores de RA

En la constitución de una nueva RA, se realizarán las siguientes acciones:

- Firmaprofesional verificará la existencia de la entidad mediante sus propias fuentes de información.
- Un representante autorizado de la organización deberá firmar un contrato con Firmaprofesional, donde se especificarán los aspectos concretos de la delegación y las responsabilidades de cada agente.

Además, se exigirá a la RA el cumplimiento de lo siguiente respecto de los operadores de RA:

- Verificar y validar la identidad de los nuevos operadores de la RA. La RA deberá enviar a Firmaprofesional la documentación correspondiente al nuevo operador, así como su autorización a que actúe como operador de RA.
- Asegurar que la validación de la identidad de un operador de la RA es realizada por una persona física diferente de dicho operador.
- Asegurar que los operadores de la RA hayan recibido formación suficiente para el desempeño de sus funciones, asistiendo como mínimo a una sesión de formación de operador.
- Asegurar que la comunicación entre la RA y Firmaprofesional se realiza de forma segura mediante el uso de certificados digitales de operador.

3.2.6 Criterios para interoperación

En la actualidad Firmaprofesional no dispone de certificación cruzada.

3.2.7 Identificación de certificados de alto riesgo

Firmaprofesional dispone de métodos de identificación de certificados de alto riesgo mediante el uso de listas negras, que requieren comprobaciones adicionales.

Las fuentes externas, como "listas negras" emitidas por el gobierno o listas internacionales de personas denegadas reconocidas que son aplicables a las jurisdicciones en las que la CA emisora se pueden utilizar para seleccionar a los solicitantes no deseados.

3.3 Identificación y autenticación en la renovación de claves

3.3.1 Renovación de certificados rutinaria

3.3.1.1 Renovación de certificados online

El firmante se podrá identificar y autenticar en el proceso de renovación online mediante un certificado cualificado si se cumple lo siguiente:

- La RA ha autorizado la renovación.
- El certificado que desea renovar no ha caducado.
- En el caso de certificados cualificados, han transcurrido menos de 5 años desde su última personación e identificación ante la RA.

Los requisitos específicos podrán diferir según el tipo de certificado solicitado y estarán recogidas en la "Política de Certificación" correspondiente.

Si alguno de los atributos o nombres certificados ha cambiado, la información de registro relacionada deberá ser verificada, registrada y aceptada por el suscriptor siguiendo REG-6.3.1-00B y la cláusula 6.2.2.

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.

3.3.2 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 en la revocación de certificados

La identificación de los firmantes en el proceso de revocación de certificados podrá ser realizada por:

a. El propio firmante: identificándose y autenticándose mediante el uso del Código de Revocación en la página web de Firmaprofesional.

b. Cualquier RA de Firmaprofesional: deberá identificar al firmante ante una petición de revocación según los propios medios que considere necesarios.

c. En caso de revocación de certificados para PSD2, sean de autenticación web o de sello electrónico, la solicitud de revocación puede ser realizada por el Banco de España o la Autoridad Nacional Competente (ANC), mediante correo electrónico a soporte@firmaprofesional.com conteniendo un PDF sellado con un certificado cualificado de sello electrónico a nombre de la ANC. El PDF debe contener los datos del certificado a revocar: al menos el DN del sujeto y el número de serie del certificado.

Firmaprofesional verificará la autenticidad de las solicitudes de revocación de certificados de PSD2 solicitadas por dichas Autoridades Competentes.

Si la ANC hubiera notificado a Firmaprofesional una dirección de correo electrónico donde pueda contactar, FIrmaprofesional informará a la ANC cómo puede autenticarse para solicitar la revocación de un certificado de PSD2.

Cada Política de Certificación definirá el proceso de revocación aplicable a los certificados emitidos bajo la misma.

4 Requisitos operacionales para el ciclo de vida de los certificados

4.1 Solicitud de certificados

4.1.1 Quién puede solicitar un certificado

Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

4.1.2 Proceso de solicitud de certificados y responsabilidades

El solicitante deberá contactar con Firmaprofesional o con un Intermediario de Firmaprofesional que actúe como RA para gestionar la solicitud del certificado.

La RA proporcionará al solicitante la siguiente información:

- Documentación necesaria a presentar para la tramitación de su solicitud y para verificar la identidad del firmante.
- Disponibilidad para realizar el proceso de registro.
- Información sobre el proceso de emisión y revocación, de la custodia de la clave privada, así como de las responsabilidades y las condiciones de uso del certificado y del dispositivo.
- Cómo poder acceder y consultar el presente documento y las políticas de certificación.

En las políticas de certificación (CP) se especifica la documentación requerida para la solicitud de cada tipo de certificado.

En el caso de que el solicitante sea una Corporación que actúe como RA de Firmaprofesional, la Corporación podrá gestionar directamente las solicitudes accediendo de forma segura a los sistemas informáticos de Firmaprofesional y generar los certificados correspondientes para la propia Corporación o para sus miembros.

4.2 Tramitación de las solicitudes de certificados

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".

La comprobación de los registros CAA se realiza automáticamente conforme a la RFC 8659.

4.2.1 Realización de las funciones de identificación y autenticación

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

En todo caso, el registro de la identidad del suscriptor se realiza siguiendo aquello establecido en el apartado 3.2 - Validación inicial de la identidad –, asegurando la validación de la identidad de suscriptor y sujeto.

El procedimiento empleado para la verificación inicial de la identidad y los atributos del sujeto continua siendo un procedimiento aplicable para dicha verificación de acuerdo con la DPC vigente en el momento de emisión del certificado.

4.2.2 Aprobación o denegación de las solicitudes de certificados

Una vez realizada la solicitud de certificado, la RA deberá verificar la información proporcionada por el solicitante, incluyendo la validación de la identidad del firmante. Además, la RA deberá verificar que las solicitudes de certificados son adecuadas, autorizadas y completas, de acuerdo con la evidencia o declaración acerca de la identidad recopilada siguiendo aquello establecido en el apartado 3.2 de esta DPC.

En el momento de la expedición del certificado, la RA deberá verificar que los atributos del sujeto, y cualquier otra información incluida en el certificado a expedir, son correctos.

Si la información no es correcta, la RA denegará la petición, contactando con el solicitante para comunicarle el motivo. Si es correcta, se procederá a la firma del instrumento jurídico vinculante entre el suscriptor y/o el solicitante y Firmaprofesional.

Se procederá entonces a la emisión del certificado.

4.2.3 Tiempo de tramitación de las solicitudes de certificado

El tiempo de tramitación de las solicitudes de certificado dependerá del proceso de verificación de la información proporcionada por el solicitante, incluyendo la validación de la identidad del firmante.

4.3 Emisión de certificados

4.3.1 Acciones de la CA durante la emisión de los certificados

Para la emisión de certificados se realizarán las siguientes acciones:

- Se generarán un par de claves de manera segura, garantizando el acceso exclusivo del firmante a los datos de generación de firma. Si la generación del par de claves la realiza el suscriptor deberá utilizar los algoritmos o suite criptográfica y tamaños de claves identificados en los apartados 7.1.3 y 6.15 respectivamente del presente documento.

- Si es necesario, la RA entregará al firmante los mecanismos necesarios para hacer uso de esos datos de generación de firma (ej, entrega física del DCCF, códigos de activación, etc ...)

- Si es necesario, el firmante entregará su clave pública a la RA.

- La RA verificará nuevamente el contenido de la petición de certificado con la documentación presentada. Si la verificación es correcta, la RA validará la petición.

- LA RA enviará por un canal seguro la clave pública del firmante junto con los datos verificados a la CA.

- La CA verificará la procedencia y la integridad de los datos enviados por la RA.

- Si todo es correcto, la CA emitirá el certificado en un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.

- Durante la generación de los certificados, la CA se encargará de añadir las informaciones restantes establecidas necesarias para cumplir con los requisitos técnicos y legales establecidos.

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

- El certificado generado será enviado a la RA, que lo pondrá a disposición del firmante.

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

La CA notificará al suscriptor y/o firmante la emisión del certificado y el método de descarga si es necesario.

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

Una vez el certificado esté generado y aceptado por el suscriptor o firmante, podrá ser publicado en los repositorios de certificados que se consideren necesarios.

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

En caso de emisión de certificados de PSD2, si Firmaprofesional ha sido notificado sobre la dirección de correo electrónico de la ANC identificada en el certificado de nueva emisión, Firmaprofesional remitirá a dicha dirección de correo electrónico la información del contenido del certificado incluyendo el número de serie del certificado en formato hexadecimal, el sujeto el nombre distinguido del sujeto, el nombre distinguido del emisor, el período de validez del certificado, así como la información de contacto y las instrucciones para las solicitudes de revocación y una copia del archivo del certificado.

4.5 Uso de las claves y el certificado

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

Los certificados podrán ser utilizados según lo estipulado en esta CPS y en la Política de Certificación y Texto de Divulgación-PDS correspondientes.

La extensión Key Usage podrá ser utilizada para establecer límites técnicos a los usos de la clave privada del certificado correspondiente. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas de terceros, quedando su regulación fuera del alcance de este documento.

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

Los terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente CPS y la Política de Certificación correspondiente.

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

4.6 Renovación de certificados sin cambio de claves

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

4.6.1 Circunstancia para la renovación del certificado

Sin estipulación.

4.6.2 Quién puede solicitar la renovación

Sin estipulación.

4.6.3 Proceso de solicitudes de renovación de certificados

Sin estipulación.

4.6.4 Notificación al suscriptor de la emisión de un nuevo certificado

Sin estipulación.

4.6.5 Conducta que constituye la aceptación de un certificado de renovación

Sin estipulación.

4.6.6 Publicación del certificado de renovación por parte de la CA

Sin estipulación.

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

Sin estipulación.

4.7 Renovación del certificado con cambio de claves

Existen dos posibilidades para la renovación de certificados:

a. Proceso de renovación presencial, que se efectuará del mismo modo que la emisión de un nuevo certificado.

b. Proceso de renovación online, que se detalla a continuación:

4.7.1 Circunstancias para la renovación online con cambio de claves

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

- La RA dispone del servicio de renovación online.
- 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.
- En caso de emplear un certificado cualificado previamente emitido para autenticar la solicitud de renovación con cambio de claves, se verificará su existencia y validez.

4.7.2 Quién puede pedir la renovación online de un certificado

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

4.7.3 Tramitación de las peticiones de renovación online

El firmante podrá contactar con la RA que emitió su certificado y solicitar su renovación. La RA le informará de cómo formalizar su solicitud.

En general, para la emisión de un certificado renovado, deberán cumplirse todos los requisitos incluidos en los apartados 4.1 - Solicitud de certificados -, y 4.2 - Tramitación de las solicitudes de certificados.

Se realizarán los siguientes pasos:

- La RA recibirá una notificación de que un certificado está a punto de expirar. En ese momento, la RA podrá autorizar la renovación.
- El firmante será notificado por correo electrónico de que puede renovar su certificado.
- El firmante se conectará a la página web de Firmaprofesional y mediante el uso de su certificado, firmará la renovación de su certificado.
- Se procederá a la generación del nuevo par de claves.
- Se enviará por un canal seguro la clave pública a la CA en formato PKCS10 u otro equivalente.
- Seguidamente se realizará la generación del certificado en un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.
- El certificado generado será entregado al suscriptor.

4.7.4 Notificación de la emisión del certificado renovado

La CA notificará al suscriptor y al firmante que el certificado ha sido renovado al finalizar correctamente el proceso.

4.7.5 Forma de aceptación del certificado renovado

El certificado se aceptará al firmar electrónicamente la renovación.

4.7.6 Publicación del certificado renovado

Una vez el certificado haya sido renovado, el nuevo certificado podrá ser publicado en los repositorios de certificados que se consideren necesarios reemplazando al certificado anterior, siempre que el firmante no se hubiera opuesto.

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

Sin estipulación.

4.8 Modificación de certificados

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 de la modificación del certificado

Sin estipulación.

4.8.2 Quién puede solicitar la modificación del certificado

Sin estipulación.

4.8.3 Tramitación de solicitudes de modificación de certificados

Sin estipulación.

4.8.4 Notificación de la emisión de un nuevo certificado al suscriptor

Sin estipulación.

4.8.5 Comportamiento que constituye la aceptación de un certificado modificado

Sin estipulación.

4.8.6 Publicación del certificado modificado por la AC

Sin estipulación.

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

Sin estipulación.

4.9 Revocación y suspensión de certificados

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible.

La suspensión supone la pérdida temporal de validez de un certificado, y es reversible.

Las revocaciones y suspensiones tienen efecto desde el momento en que aparecen publicadas en la CRL.

4.9.1 Circunstancias para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

a. Circunstancias que afectan a la información contenida en el certificado:

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
- Pérdida del firmante de condición de colegiado, en el caso de Certificados Corporativos de Colegiado.
- Pérdida o cambio de la vinculación del firmante con la Corporación.
- Se ha revocado el rol del proveedor del servicio de pago incluído en el certificado de PSD2.

b. Circunstancias que afectan a la seguridad de la clave privada o del certificado:

- Compromiso de la clave privada o de la infraestructura o sistemas de la CA, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción, por parte de la CA o de la RA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la CPS y Política de Certificación pertinente.
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor.

- Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor.
- El uso irregular del certificado por el suscriptor o firmante.
- La CA conoce un método demostrado o comprobado que puede calcular fácilmente la clave privada del suscriptor en función de la clave pública en el certificado.

c. Circunstancias que afectan a la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del suscriptor.

d. Circunstancias que afectan al suscriptor o firmante:

- El incumplimiento por parte del suscriptor o firmante de las normas de uso del certificado expuestas en la presente CPS o en el instrumento jurídico vinculante entre Firmaprofesional y el suscriptor.
- Finalización de la relación jurídica entre la Firmaprofesional y el Suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al firmante, incluyendo la inhabilitación temporal del colegiado para el ejercicio profesional.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
- Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en la CPS.
- La incapacidad sobrevenida, total o parcial.
- Por el fallecimiento del suscriptor o firmante.
- La recepción de una solicitud de revocación válida, por cualquier causa, emitida por el suscriptor o firmante.

- La autorización para ser proveedor de servicios de pago ha sido revocada por la ANC.

e. Otras circunstancias:

- La suspensión del certificado digital por un período superior al establecido en la CPS.
- Por resolución judicial o administrativa que lo ordene.
- Para los certificados SSL, por cualquiera de las causas establecidas en los Baseline Requirements o en los EV Guidelines del CA Browser Forum y en los tiempos establecidos para cada causa.
- Cualquier circunstancia establecidas en las MRSP.
- Por la concurrencia de cualquier otra causa especificada en la CPS y en la legislación vigente.

4.9.2 Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

- El propio firmante, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.
- Cualquier persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.
- En caso de revocación de certificados de PSD2, la solicitud de revocación puede ser realizada por el Banco de España o la Autoridad Nacional Competente (ANC)

En todo caso, la ANC podrá especificar en su solicitud la razón por la que solicita la revocación.

Podrán tramitar la revocación del certificado:

- Los operadores de la RA del Suscriptor del certificado.
- Los operadores autorizados de la CA.

4.9.3 Procedimientos de solicitud de revocación

Existen distintas alternativas para el suscriptor o el firmante a la hora de solicitar la revocación del certificado.

En todo caso, al tiempo de suspenderse o revocarse el certificado, se enviará un comunicado al firmante, comunicando la fecha, hora y la causa de la misma.

4.9.3.1 Procedimiento online

Firmaprofesional pondrá a disposición del suscriptor o del firmante un formulario web desde el que podrá solicitar la revocación de su certificado. Este mecanismo de solicitud de revocación se convierte en el principal para todos los certificados emitidos por cualquier Operador de RA, de tal forma que se garantiza que cualquier certificado puede realizarse su revocación en menos de 24 horas. Para ello, el suscriptor deberá:

- Acceder a la web de Firmaprofesional en el apartado correspondiente a revocación.
- En el formulario dispuesto, escribir correctamente sus datos que le identifique.
- Introducir el Código de Revocación proporcionado durante el proceso de generación del certificado.
- Aceptar explícitamente la tramitación de la solicitud y las consecuencias de ésta.

Una vez aceptada la tramitación, el certificado será inmediatamente revocado.

La RA recibirá un correo del sistema informándole que se ha producido la revocación del certificado.

En caso de que la RA no pueda confirmar el estado de revocación en 24 horas, se registran todas las acciones emprendidas junto con la justificación de las mismas.

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

4.9.5.1 Revocación en horario de oficina

El suscriptor o el firmante deberá ponerse en contacto con su RA, y ésta, a su vez, deberá identificar y autenticar su identidad mediante los procedimientos que considere oportunos.

Una vez correctamente identificado, el operador procederá a efectuar la revocación.

4.9.5.2 Revocación fuera de horario de oficina

Para solicitar la revocación de un certificado telefónicamente fuera de horario de oficina se deberá contactar con el servicio de revocación telefónica de Firmaprofesional al número siguiente:

- Servicio de revocación 24x7: 902.361.639

Firmaprofesional suspenderá preventivamente el certificado, antes de 24 horas tras recibir la petición de revocación, y enviará un mensaje a la RA con los datos de la suspensión y el motivo.

La RA dispondrá de un máximo de 5 días para verificar la veracidad de la solicitud de revocación y poder así completar, o en caso contrario cancelar, el proceso de revocación del certificado.

Este plazo será de 24 horas en el caso de que:

- el suscriptor solicite por escrito que Firmaprofesional revoque el certificado;
- el suscriptor notifique a Firmaprofesional que no autorizó la solicitud original del certificado y no concede retroactivamente la autorización;
- Firmaprofesional obtiene pruebas de que la clave privada del suscriptor correspondiente a la clave pública en el certificado sufrió un compromiso clave;
- Firmaprofesional obtiene evidencia de que no se debe confiar en la validación de la autorización de dominio o control de cualquier nombre de dominio cualificado o dirección IP en el certificado.

Si transcurrido este plazo, el certificado se encontrase aún suspendido, Firmaprofesional procedería a su revocación automática.

Una vez la identidad del firmante haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por la RA, la revocación se hará efectiva inmediatamente.

4.9.6 Obligación de verificación de las revocaciones por los terceros

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

4.9.7 Frecuencia de emisión de CRLs

La CRL de los certificados de entidad final se emite al menos cada 24 horas, o cuando se produzca una revocación en el intervalo de los 30 minutos siguientes a la misma, con una validez de 7 días.

La CRL de los certificados de autoridad se emite cada 6 meses o cuando se produzca una revocación.

La inconsistencia entre la información del OCSP y la CRL se produce debido a que el OCSP se actualiza de manera previa a la CRL. La información válida será la que proporcione el sistema en línea de verificación del estado de los certificados (OCSP).

En cualquier caso, la CRL no contiene los certificados caducados, por lo que en caso de consulta sobre el estado de un certificado caducado la información válida será la que proporcione el sistema en línea de verificación del estado de los certificados (OCSP)

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

Dado que la publicación de las CRL se realiza en el momento de la generación de la misma, se considera cero o nulo el tiempo transcurrido.

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

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la CA, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

4.9.10 Requisitos de comprobación de revocación en línea

Para el uso del servicio de CRLs, que es de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión "CRL Distribution Point".
- El usuario deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren serán retirados de la CRL.

Para usar el servicio OCSP, se debe considerar lo siguiente:

- Las revocaciones se pueden verificar utilizando los métodos GET o POST.
- La información proporcionada a través del servicio OCSP se actualiza al menos cada cuatro días.

4.9.11 Otras formas de anuncios de revocación disponibles

Sin estipulación.

4.9.12 Necesidades especiales en relación con un compromiso de clave

Ver sección 4.9.1.

Adicionalmente, Terceras partes pueden utilizar los siguientes métodos para demostrar un posible compromiso de claves:

- Enviar un CSR firmado, la clave privada que ha sido comprometida u otra respuesta de desafío firmada por dicha Clave privada y verificable por la clave pública.
- Proporcionar referencias a fuentes de incidentes de seguridad y / o vulnerabilidad por las cuales el compromiso sea verificable.
- Enviar binarios que contienen una clave privada comprometida, incluido el método para extraer la clave privada.

Firmaprofesional analizará otros posibles métodos o solicitudes y actualizará el CPS en consecuencia si el nuevo método se acepta y es verificable el posible compromiso de claves.

4.9.13 Circunstancias para la suspensión

Firmaprofesional podrá suspender un certificado en los casos siguientes:

- Si se sospecha el compromiso de una clave, hasta que este hecho sea confirmado o desmentido.
- Si el suscriptor ha incurrido en falta de pago de su certificado.
- Si no disponen de toda la información necesaria para determinar la revocación de un certificado.

4.9.14 Quién puede solicitar la suspensión

Solamente podrán realizar la suspensión del certificado:

- Los operadores de la RA del Suscriptor del certificado.
- Los operadores autorizados de la CA.

4.9.15 Procedimiento de solicitud de suspensión

Existen distintas alternativas para el suscriptor o el firmante a la hora de solicitar la suspensión del certificado.

4.9.16 Límites del periodo de suspensión

Al cabo de 15 días de suspensión, la CA podrá proceder a la revocación del certificado.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

Firmaprofesional ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

Firmaprofesional ofrece un servicio gratuito de acceso a validación de certificados en línea por medio del protocolo OCSP, excepto si la CA emisora pública una última CRL (lastCRL). En este caso el estado de los certificados emitidos por la citada CA sólo se ofrecerá mediante mediante consulta a la lastCRL.

Adicionalmente, Firmaprofesional puede ofrecer servicios comerciales de validación de certificados.

4.10.2 Disponibilidad del servicio

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la CA, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

En caso de cese de la actividad y/o caducidad o compromiso de claves de la CA, se generará una última CRL (lastCRL) que se mantendrá íntegra y disponible para su consulta garantizando la disponibilidad del servicio de información sobre el estado de los certificados, durante al menos 15 años desde su publicación.

La provisión de la información sobre el estado de revocación de los Certificados, en caso de cese de actividad de Firmaprofesional como Prestador de Servicios de Confianza, queda garantizada mediante la transferencia, al organismo supervisor o a otro Prestador con el que se llegue al correspondiente acuerdo, de toda la información relativa a los Certificados y, especialmente, de los datos de su estado de revocación.

Firmaprofesional mantiene una capacidad continua 24x7 para responder internamente a un certificado de alta prioridad, informando del problema y, en su caso, reenviando dicha queja a las autoridades policiales, y / o revocando un certificado que sea objeto de dicha queja.

4.10.3 Características adicionales

La utilización del servicio OCSP es público y gratuito. La información sobre el estado de revocación o caducidad de los Certificados permite a los usuarios conocer el estado del Certificado, no solo hasta que éste expire, sino más allá de dicha fecha, a través del servicio de OCSP.

Firmaprofesional puede disponer de servicios avanzados de validación de certificados que requiera de una licencia específica.

4.11 Finalización de la suscripción

La suscripción finalizará en el momento de expiración o revocación del certificado.

4.12 Custodia y recuperación de claves

Firmaprofesional no custodia copias de respaldo de las claves privadas de los suscriptores y firmantes ni ofrece servicios de recuperación de claves (key escrow).

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

La CA tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación y revocación de certificados ofrece protección frente:

- Accesos físicos no autorizados.
- Desastres naturales.
- Incendios.
- Fallo de los sistemas de apoyo (energía eléctrica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Robo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Confianza.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo 24h-365 días al año con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones

garantiza la presencia de fuerzas de seguridad en un plazo no superior a 30 minutos, al encontrarse en el centro urbano de una capital de provincia.

5.1.1 Ubicación física y construcción

Las instalaciones de la CA están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, y ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una jaula de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

5.1.2 Acceso físico

El acceso físico a las dependencias del Prestador de Servicios de Confianza donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables, así como sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

El acceso a las salas se realiza con lectores de tarjeta de identificación y huella dactilar, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.

5.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones de la CA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicados mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 Exposición al agua

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Protección y prevención de incendios

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

5.1.6 Sistema de almacenamiento

Cada medio de almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información que contenga y permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento, se guarda en armarios ignífugos o bajo llave permanentemente, requiriéndose autorización expresa para su retirada.

5.1.7 Eliminación de los soportes de información

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga:

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.
- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

5.1.8 Copias de seguridad fuera de las instalaciones

La CA mantiene un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos independiente del centro operacional.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2 Controles de procedimiento

5.2.1 Roles de confianza

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de la jerarquía de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación.

Según lo especificado en las normas ETSI EN 319 401 y CEN/TS 419261, los roles mínimos establecidos son:

a. **Responsable de seguridad (Security Officer)**: Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.

b. **Operador de RA (Registration Officer)**: Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final, así como las oportunas verificaciones en certificados de autenticación web.

c. **Responsable de revocación (Revocation Officers):** Responsable de realizar los cambios en el estado de un certificado.

d. **Administradores del sistema de certificación (System Administrators):** Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.

e. **Operadores de sistemas (System Operators):** Responsables de la gestión del día a día del sistema (Monitorización, backup, recovery…)

f. **Auditor interno de Sistemas (System Auditors):** Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.

g. **Operador de CA - Operador de Certificación:** Responsables de activar las claves de la CA en el entorno Online, o de los procesos de firma de certificados y CRL's en el entorno Root Offline.

5.2.2 Número de personas requeridas por tarea

La CA garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

- La generación de la clave de las CA's.
- La recuperación y back-up de la clave privada de las CA's.
- La emisión de certificados de las CA's.
- Activación de la clave privada de las CA's.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la root CA.

5.2.3 Identificación y autenticación por rol

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.

Cada persona sólo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

5.2.4 Roles que requieren segregación de funciones

Las tareas de Auditor Interno de Sistemas son incompatibles en el tiempo con las tareas de Operador de Certificación e incompatibles con las tareas de Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

5.3 Controles de personal

5.3.1 Requisitos relativos a la calificación, conocimiento y experiencia profesionales

Todo el personal que realiza tareas calificadas como confiables sin supervisión, lleva al menos seis meses trabajando en el centro de producción y tiene contrato laboral fijo.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

Tanto los ejecutivos de Firmaprofesional como el personal con roles de confianza están libres de cualquier presión comercial, financiera u de otra índole que pudiere influir negativamente en la confianza en los servicios que presta.

En los casos en que el suscriptor actúe como autoridad de registro, el Colegio profesional/Administración Pública, organismo o entidad de derecho público/empresa de que se trate, designa de entre su personal al personal habilitado para la realización de las funciones de registro, designación la cual se realiza por medio del responsable del servicio de certificación, previamente identificado en el Contrato de prestación de servicios de certificación electrónica.

El empleado del registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las peticiones. Al final de dicho curso, un auditor externo procederá a evaluar sus conocimientos del proceso.

Los especialistas de validación deberán cumplir los requisitos previos de formación y cualificación establecidos en el apartado 14.1.2 de los EV Guidelines y el apartado 5.3.3 de los Baseline Requirements del CA/Browser Forum.

Firmaprofesional retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

5.3.2 Procedimientos de comprobación de antecedentes

Firmaprofesional realiza las investigaciones pertinentes antes de la contratación de cualquier persona.

Las RA pueden establecer criterios diferentes, siendo responsables por la actuación de las personas que autoricen.

5.3.3 Requerimientos de formación

Firmaprofesional realiza los cursos necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y en función de los conocimientos personales de cada operador.

5.3.4 Requerimientos y frecuencia de actualización de la formación

Se realizarán actualizaciones con una frecuencia anual, salvo por modificaciones a la CPS, que serán notificadas a medida que sean aprobadas.

5.3.5 Frecuencia y secuencia de rotación de tareas

Sin estipulación.

5.3.6 Sanciones por actuaciones no autorizadas

Firmaprofesional dispone de un régimen sancionador interno para sancionar la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

5.3.7 Requisitos de contratación de terceros

Los empleados contratados para realizar tareas confiables deberán firmar con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por la CA. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

En cualquier caso, deberán cumplir los mismos requerimientos exigidos para un trabajador de Firmaprofesional, tanto de formación previa como de cualificación de habilidades, para la realización de funciones específicas de operador o especialistas de validación.

5.3.8 Documentación proporcionada al personal

Firmaprofesional pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

Firmaprofesional registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la CA. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la CA a través de la red.
- Intentos de accesos no autorizados a la red interna de la CA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la Autoridad de Certificación.
- Encendido y apagado de la aplicación de la CA.
- Cambios en los detalles de la CA y/o sus claves.
- Cambios en la creación de perfiles de certificados.

- Generación de claves propias.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico de la CA.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, Firmaprofesional registra:

- Los cambios en la política de seguridad
- Los colapsos del sistema
- Los fallos en el hardware
- Las actividades de los cortafuegos y enrutadores.
- La documentación presentada por el solicitante, así como toda la información del proceso de registro.
- Todos los sucesos relacionados con la preparación de los dispositivos DCCF

Firmaprofesional conserva, ya sea manual o electrónicamente, la siguiente información:

- Las ceremonias de creación de claves de las CA y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal que realiza tareas de confianza en la CA.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de las CA.

Solo las personas autorizadas por Firmaprofesional tendrán acceso a esta documentación.

5.4.2 Frecuencia de procesado de registros de auditoría

Se revisarán los logs de auditoría cada semana y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

5.4.3 Periodo de conservación de los registros de auditoría

Se almacenará la información de los logs de auditoría durante 15 años para garantizar la seguridad del sistema.

5.4.4 Protección de los registros de auditoría

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la Autoridad de Certificación.

Los dispositivos son manejados en todo momento por personal autorizado.

5.4.5 Procedimientos de respaldo de los registros de auditoría

Firmaprofesional dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

La CA tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena en armario ignífugo bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado. Se realizan copias diarias incrementales y completas semanales.

Adicionalmente se mantiene copia de los logs de auditoría en centro de custodia externo.

5.4.6 Sistema de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

5.4.7 Notificación al sujeto causante del evento

Sin estipulación

5.4.8 Análisis de vulnerabilidades

La CA realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, test de intrusión (anual) así como análisis de vulnerabilidades (trimestrales) de direcciones IP internas y externas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

5.5 Archivo de registros

5.5.1 Tipo de eventos archivados

Se conservarán los eventos que tengan lugar durante el ciclo de vida del certificado, incluyendo la renovación del mismo. Se almacenará por la CA o, por delegación de ésta en la RA:

- todos los datos de la auditoría,
- todos los datos relativos a los certificados, incluyendo los contratos con los suscriptores y los datos relativos a su identificación,
- solicitudes de emisión y revocación de certificados,
- todos los certificados emitidos o publicados,
- CRL's emitidas o registros del estado de los certificados generados,
- la documentación requerida por los auditores y
- las comunicaciones entre los elementos de la PKI

La CA es responsable del correcto archivo de todo este material y documentación.

5.5.2 Periodo de conservación de registros

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados se conservarán publicados en el repositorio durante al menos un año desde su expiración. Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos 15 años a contar desde el momento de la caducidad o revocación del certificado) y, en todo caso, durante el periodo que establezca la legislación vigente.

5.5.3 Protección del archivo

La CA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

La CA dispone de documentación técnica y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

5.5.4 Procedimientos de copia de seguridad del archivo

La CA dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo a personal autorizado.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable.

Existe dentro de la documentación técnica y de configuración de la CA un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

5.5.6 Sistema de archivo de información de auditoría

Sin estipulación.

5.5.7 Procedimientos para obtener y verificar información archivada

Durante la auditoría requerida por esta CPS, el auditor verificará la integridad de la información archivada.

El acceso a la información archivada se realiza sólo por personal autorizado.

La CA proporcionará la información y los medios al auditor para poder verificar la información archivada.

5.6 Cambio de claves de la CA

5.6.1 CA Raíz

Antes de que el certificado de la CA Raíz expire se realizará un cambio de claves (rekeying) y, en su caso, se introducirán cambios en el contenido del certificado que se ajusten mejor a la legislación vigente y la realidad de Firmaprofesional y del mercado. La CA antigua y su clave privada sólo se usarán para la firma de CRL's mientras existan certificados activos emitidos por la CA antigua. Se generará una nueva CA con una clave privada nueva.

La documentación técnica y de seguridad de la CA detalla el proceso de cambio de claves de la CA.

5.6.2 CA Subordinada

En el caso de las CA subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves. Sólo cuando se realice el cambio se aplicará lo descrito en el punto anterior.

5.7 Plan de recuperación de desastres

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

La CA ha desarrollado un plan de contingencias, detallado en el documento "Política de Seguridad", para recuperar todos los sistemas en menos de 48 horas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la CA para implementar dichos procesos.

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

En el caso de que tuviera lugar un incidente que alterase o corrompiese tanto recursos hardware, software como datos, Firmaprofesional procederá según lo estipulado en el documento "Política de seguridad".

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

El Plan de Continuidad de la jerarquía de Firmaprofesional trata el compromiso de la clave privada o de la suite criptográfica (algoritmos) utilizada de la CA como un desastre.

En caso de compromiso de la clave privada de la CA, Firmaprofesional:

1. Informará de este caso a todos los suscriptores, usuarios y otras CA's con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de la CA.

2. Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave o algoritmos no son válidos.

3. En el caso de que hubiese un compromiso de clave se facilitará/publicará un hash de la última CRL en https://crl.firmaprofesional.com/.

4. Notificará al supervisor nacional en un plazo de 24 horas tras tener conocimiento del compromiso

5. Notificará a los fabricantes de software que confían en los certificados en los plazos establecidos en las respectivas políticas de admisión de autoridades de certificación.

6. Revocará, en el plazo que se pacte con el supervisor nacional, los certificados emitidos por esta CA, aplicando, si procede, alguno de los procedimientos previstos en el Plan de Cese o en el Plan de Continuidad.

5.7.4 Continuidad del Negocio después de un desastre

La CA restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con esta CPS dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

La CA dispone de un centro alternativo, en caso de ser necesario, para la puesta en funcionamiento de los sistemas de certificación.

5.8 Cese de actividad

5.8.1 Autoridad de Certificación

Antes del cese de su actividad la CA realizará las siguientes actuaciones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación hasta el cese definitivo de la actividad, si es el caso.

- Informará a todos los suscriptores, solicitantes, usuarios, otras CA's o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.

- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la CA en el procedimiento de emisión de certificados.

- De acuerdo con el artículo 9.3.c) de la Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza , la CA podrá transferir una vez

acreditada la ausencia de oposición de los suscriptores , la gestión de los certificados que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de confianza que los asuma o, en caso contrario, extinguir su vigencia. La CA informará, cuando sea el caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quien.

- Con carácter previo al cese definitivo de la actividad, comunicará a la administración competente la información relativa a los certificados cualificados expedidos al público cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 9.3.a) de la Ley 6/2020.

- Informará a la administración competente, la apertura de cualquier proceso concursal que se siga contra Firmaprofesional, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

- Firmaprofesional indica en su plan de finalización del servicio qué información será retornada.

5.8.2 Autoridad de Registro

Ante el cese de una autoridad de registro de un colectivo específico, Firmaprofesional:

- Dejará de emitir y renovar certificados de esa RA.

- Revocará los certificados de operador de esa RA.

- Revocará los certificados de suscriptor emitidos por esa RA salvo que expresamente se decida lo contrario.

A su vez, la RA:

- Entregará toda la documentación asociada a la emisión y gestión de los certificados, ya sea en formato papel, electrónico o cualquier otro, a Firmaprofesional.

6 Controles de seguridad técnica

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

La generación de la clave de las CAs se realiza, de acuerdo con el proceso documentado de ceremonia de claves, dentro de la sala de seguridad del PSC, en dispositivos criptográficos hardware (HSM), por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de Firmaprofesional, de la organización titular de la CA y del auditor.

Firmaprofesional garantiza que las claves de firma de la CA no son empleadas para otro supuesto que los indicados en este documento.

Para los certificados de entidad final, la generación de claves se realizará en dispositivos que aseguren razonablemente que la clave privada únicamente puede ser utilizada por el firmante, bien por medios físicos, bien estableciendo el suscriptor los controles y medidas de seguridad adecuadas.

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) que cumpla con los requisitos establecidos en el Anexo II del Reglamento UE 910/2014, se indicará en el propio certificado mediante la inclusión del identificador OID correspondiente en la extensión "Certificate Policies".

En cualquier otro caso, por ejemplo, si las claves privadas han sido generadas en un navegador de Internet, los certificados se emitirán con un identificador OID diferente.

6.1.2 Entrega de la clave privada al firmante

La RA será responsable de garantizar la entrega del certificado al firmante, ya sea entregándole el dispositivo de firma o habilitándole los mecanismos para su descarga y posterior uso, asegurándose así que este último está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

6.1.3 Entrega de la clave pública al emisor del certificado

El envío de la clave pública a la CA para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X.509 autofirmado, utilizando un canal seguro para la transmisión.

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

El certificado de las CAs de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en la página web de Firmaprofesional.

6.1.5 Tamaño de las claves

Certificado	Tamaño claves RSA (bits)	Tamaño Claves ECC	Periodo validez (años)
CA Raíz	4096	ECC P-384	25
CA Subordinadas	2048	ECC P-384	25
Entidad final	2048		Lo establecido en la legislación y normativa vigentes
Operador / Administrador	2048		5 (máximo)

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

Se utilizan los parámetros recomendados en el documento de especificaciones técnicas de la ETSI TS 119 312.

Concretamente los parámetros utilizados son los siguientes:

Signature Suite	Hash Function	Padding Method	Signature algorithm
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa
ecdsa-with-SHA384	SHA384		ecdsa

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

Todos los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de las claves y limitando técnicamente la funcionalidad del certificado en el software compatible con X.509v3.

La matización de estos usos o limitaciones, si se considera necesario, estarán definidas en la Política de Certificación correspondiente.

Las Claves Privadas correspondientes a Certificados Raíz no se utilizarán para firmar Certificados excepto en los siguientes casos:

- Certificados autofirmados para representar a la propia CA raíz;
- Certificados para CA subordinadas y certificados cruzados;
- Certificados para verificación de respuesta OCSP.

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

6.2.1 Estándares para los módulos criptográficos

Los módulos criptográficos empleados para generar y almacenar las claves de las Autoridades de Certificación ha sido validado para cumplir con al menos FIPS 140-2 nivel 3, FIPS 140-3 nivel 3, o un perfil de protección de common criteria apropiado o un objetivo de seguridad, EAL 4 (o superior).

Las claves de los suscriptores de certificados cualificados con DCCF, que cumple lo establecido en la Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, al artículo 39, apartado 2, y al artículo 51.1 del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y las claves de operadores y administradores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico

seguro. Firmaprofesional verifica que los dispositivos criptográficos (DCCF) tanto si los aporta Firmaprofesional como si los aporta el suscriptor, cumplen los requisitos apropiados por la normativa y legislación vigente. Esta verificación también se realiza a lo largo del tiempo.

En el caso de que se vaya a producir una pérdida de cualificación de alguno de los dispositivos usados por Firmaprofesional como QSCD, se procederá a la búsqueda de proveedores sustitutivos de dichos dispositivos, se dejará de emplear dicho dispositivo antes de la pérdida de la cualificación y se notificará a los clientes la futura pérdida de cualificación para tomar las medidas oportunas. En cualquier caso, Firmaprofesional revocará todos los certificados vigentes que hubiesen sido emitidos en aquellos dispositivos que hayan perdido la cualificación.

Firmaprofesional no responderá de los perjuicios que la pérdida de cualificación de los dispositivos cualificados de creación de firma (tarjeta, token o HSM) y la consecuente y obligada revocación de los certificados pudiese ocasionar al usuario o a terceros. El CLIENTE conoce y acepta que los dispositivos cualificados de creación de firma (tarjeta o token) no podrán ser reutilizados una vez que caduquen los certificados.

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

El acceso a las claves privadas de las CA requiere el concurso simultáneo de dos dispositivos criptográficos diferentes de cinco posibles, protegidos por una clave de acceso.

6.2.3 Custodia de la clave privada

La clave privada de la CA raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

Las claves privadas de las CA Subordinadas están custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3.

Cuando Firmaprofesional custodia la clave privada de los suscriptores éstas están custodiadas por un dispositivo criptográfico hardware certificado EAL4+, garantizando que la misma nunca está en claro fuera del dispositivo criptográfico y que la activación y uso de dicha clave sólo puede ser realizada por el firmante.

Si el suscriptor custodia las claves privadas del firmante, deberá realizarlo utilizando dispositivos criptográficos seguros certificados según las indicaciones expuestas en el punto 6.2.1 y garantizando en todo momento el uso exclusivo de las claves por parte del firmante.

6.2.4 Copia de seguridad de la clave privada

Existen unos dispositivos que permiten la restauración de la clave privada de la CA, que son almacenados de forma segura y sólo accesibles por personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro.

Las claves de la CA Raíz y CA Subordinada se pueden restaurar por un proceso que requiere la utilización simultánea de 2 de 5 dispositivos criptográficos (tarjetas).

Este procedimiento se describe en detalle en las políticas de seguridad de Firmaprofesional.

6.2.5 Archivo de la clave privada

La CA no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de la CA para comunicarse entre sí, firmar y cifrar la información serán archivadas por un periodo de al menos 10 años, después de la emisión del último certificado.

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

Existe un documento de ceremonia de claves de la CA donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Según lo especificado en el punto 6.2.3.

6.2.8 Método de activación de la clave privada

Las claves de la CA Raíz se activan por un proceso que requiere la utilización simultánea de 2 de 4 dispositivos criptográficos (tarjetas).

Las claves de las CA Subordinadas se activan por un proceso que requiere la utilización de 1 de 4 dispositivos criptográficos (tarjetas).

6.2.9 Método de desactivación de la clave privada

Cada vez que se reinicie la aplicación las claves privadas se desactivarán automáticamente.

6.2.10 Método de destrucción de la clave privada

Firmaprofesional dispone un procedimiento de destrucción de claves privadas según las instrucciones del fabricante del módulo criptográfico de seguridad, de forma que no resulten afectadas el resto de claves gestionadas por el dispositivo, y que como mínimo requiere la presencia de un auditor, un testigo de Firmaprofesional y del Responsable de Seguridad de la Compañía.

La destrucción de claves se realizará en el propio módulo criptográfico de seguridad y en las copias de seguridad.

6.2.11 Clasificación de los módulos criptográficos

Ver apartado 6.2.1

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

La CA conservará todas las claves públicas durante el período exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación esté activo y 6 meses más como mínimo, en otro caso.

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

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

Un certificado no debe ser usado después del periodo de validez del mismo, aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación en línea válido para ese certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Los datos de activación son generados en el momento de inicialización del dispositivo criptográfico.

Si la inicialización se produce en una entidad externa, los datos de activación le serán entregados al suscriptor mediante un proceso que asegure la confidencialidad de los mismos ante terceros.

6.4.2 Protección de los datos de activación

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la CA raíz y CA subordinadas.

Para los certificados de entidad final, una vez se ha hecho entrega del dispositivo y de los datos de activación, es responsabilidad del suscriptor o firmante mantener la confidencialidad de estos datos.

6.4.3 Otros aspectos de los datos de activación

Sin estipulación.

6.5 Controles de seguridad informática

La CA emplea sistemas fiables y productos comerciales para ofrecer sus servicios de confianza.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Firmaprofesional en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

La documentación técnica y de configuración de Firmaprofesional detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.5.1 Requerimientos técnicos de seguridad específicos

Cada servidor de la CA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de CA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la CA y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la CA.
- Mecanismos de recuperación de claves y del sistema de CA.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2 Evaluación de la seguridad informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en el centro de datos de Firmaprofesional.

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

La CA posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.6.2 Controles de gestión de seguridad

6.6.2.1 Gestión de seguridad

La CA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un foro para la gestión de la seguridad.

La CA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.2 Clasificación y gestión de información y bienes

La CA mantiene un inventario de activos y documentación y un procedimiento para garantizar el correcto uso y gestión de este material.

La política de seguridad de la CA detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

6.6.2.3 Operaciones de gestión

La CA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En la documentación técnica de la CA y de procedimientos del CPD se desarrolla en detalle el proceso de gestión de incidencias.

La CA dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

La CA tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.4 Tratamiento de los soportes y seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.6.2.5 Planning del sistema

El departamento técnico de la CA mantiene un registro de las capacidades de los equipos.

Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.6.2.6 Reportes de incidencias y respuesta

La CA dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.7 Procedimientos operacionales y responsabilidades

La CA define actividades asignadas a personas con un rol de confianza distinto a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.8 Gestión del sistema de acceso

La CA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a. Gestión general de la CA:

- Se dispone de controles basados en firewalls de alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- La CA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- La CA dispone de un procedimiento para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.
- El personal de la CA será responsable de sus actos, por ejemplo, por retener logs de eventos.

b. Generación del certificado:

- Las instalaciones de la CA están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.
- La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la CA.

c. Gestión de la revocación:

- Las instalaciones de la CA están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular al sistema de revocaciones.

- La revocación se refiere a la pérdida de efectividad de un certificado digital de forma permanente. La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de CA.

d. Estado de la revocación

- La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.6.3 Gestión del ciclo de vida del hardware criptográfico

- La CA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.

- El Hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.

- La CA registra toda la información pertinente del dispositivo para añadir al catálogo de activos de Firmaprofesional, S.A.

- El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

- Firmaprofesional realiza pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

- El dispositivo criptográfico solo es manipulado por personal confiable.

- La clave privada de firma de la CA almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.

- La configuración del sistema de la CA, así como sus modificaciones y actualizaciones son documentadas y controladas.

- La CA posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7 Controles de seguridad de la red

Firmaprofesional sigue las mejores prácticas para securizar sus redes. Por ejemplo, la CA protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras se realiza de forma cifrada.

Todo lo anterior no sólo se verifica en las auditorías anuales eIDAS, sino también en las auditorias ISO 27.001, de cuya certificación dispone Firmaprofesional.

6.8 Fuente de tiempo

El tiempo se obtiene mediante un hardware específico con reloj atómico de átomo de rubidio, sincronización GPS y consulta al Real Observatorio de la Armada, siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en el RFC 5905 "Network Time Protocol".

7 Perfiles de los certificados, CRL y OCSP

7.1 Perfil de los certificados

El perfil de los certificados se corresponde con el propuesto en las políticas de certificación correspondientes, y son coherentes con lo dispuesto en las normas siguientes:

- ETSI 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles

- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 "Qualified Certificates Profile".

El perfil común a todos los certificados es el siguiente:

Campo del certificado	Nombre	Descripción
Version	N° de versión	V3 (versión del estándar X509)
Serial	n° de serie	Código aleatorio único con respecto al DN del emisor, con una entropía superior a 64 bits.
Issuer	Emisor	DN de la CA que emite el certificado
notBefore	Válido desde	Fecha de inicio de validez, tiempo UTC
notAfter	Válido hasta	Fecha de fin de validez, tiempo UTC
Subject	Asunto (DN)	Nombre distinguido del suscriptor.
Extensions …	Extensiones	Extensiones de los certificados.

7.1.1 Número de versión

Los certificados siguen el estándar X.509 versión 3.

7.1.2 Extensiones de los certificados

Extensión	Crítica	Posibles Valores
X509v3 Basic Constraints	Sí	2 valores posibles en función de si se trata de un certificado de CA: CA:FALSE CA:TRUE

X509v3 Key Usage	Sí	Variable según el tipo de certificado: Digital Signature Content Commitment Key Encipherment (1) Data Encipherment (2) Key Agreement
X509v3 Extended Key Usage	-	Variable según el tipo de certificado: serverAuth clientAuth Adobe Authentic Documents Trust emailProtection (3) timeStamping OCSPSigning
X509v3 Subject Key Identifier	-	id de la clave pública del certificado, obtenido a partir del hash de la misma
X509v3 Authority Key Identifier	-	id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma
X509v3 CRL Distribution Points	-	URI de la CRL
X509v3 Certificate Policies	-	OID de la política de certificación propia de Firmaprofesional correspondiente al certificado. URI de la CPS User Notice : Nota de texto que se puede desplegar en la pantalla del usuario (4) Cuando sea de aplicación, OID de la política europea. Cuando sea de aplicación, OID de la política española (de empleado público, de representante legal, etc).

1 Eliminado en los certificados de autenticación web

2 Eliminado en los certificados de autenticación web
3 Eliminado en todos los certificados de persona física y sellos de persona jurídica
4 Eliminado en los certificados de autenticación web

QcStatements	-	Variable según el tipo de certificado
X509v3 Subject Alternative Name	-	(opcional)
X509v3 Issuer Alternative Name	-	(opcional) URI: http://www.firmaprofesional.com
X509v3 Authority Information Access	-	URI donde se encuentra el certificado de la CA URI del servicio OCSP

Las extensiones aquí presentadas corresponden con todas las que pueden contener los certificados emitidos. Por motivos históricos y de compatibilidad, algunos certificados emitidos contienen extensiones obsoletas. En el documento "Perfiles de Certificados" se especificará las extensiones requeridas para cada tipo de certificado.

7.1.3 Identificadores de objeto (OID) de los algoritmos utilizados

OID	Nombre	Descripción
1.2.840.113549.1.1.1	rsaEncryption	OID de Clave pública
1.2.840.113549.1.1.5	sha1withRSAencryption	OID del algoritmo de firma[5]
1.2.840.113549.1.1.11	sha256withRSAencryption	OID del algoritmo de firma
1.3.132.0.34	P-384 (secp384r1)	OID de curvas elípticas
1.2.840.10045.4.3.3	ecdsa-with-SHA384	OID del algoritmo de firma

Firmaprofesional declara que las claves del firmante o suscriptor creadas por la CA son generadas usando un algoritmo reconocido como apropiado para los usos identificados en esta CPS o en la correspondiente CP, durante el tiempo de validez del mismo.

[5] Prohibido su uso desde el 1 de enero de 2016

7.1.4 Formatos de nombres

Los siguientes valores son comunes a todos los certificados de persona física:

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y Apellidos del firmante. Adicionalmente, podrá contener un código numérico de identificación, o el NIF del firmante, distinguiéndose el valor mediante la inclusión previa de una etiqueta "/num.:" o " – NIF ". Adicionalmente, podrá contener en algún tipo de certificado, indicaciones de uso "firma", "cifrado" o "autenticación".
ST, State	Ubicación Geográfica	Variable según la Política de Certificación. Ámbito geográfico de vinculación del firmante
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF o NIE del Firmante En los tipos de certificado con seudónimo este campo está prohibido.
SN, surName	Apellidos	Apellidos del Firmante En los tipos de certificado con seudónimo este campo está prohibido.
GN, givenName	Nombre de Pila	Nombre del Firmante En los tipos de certificado con seudónimo este campo está prohibido.

7.1.5 Restricciones de los nombres

Respecto a la codificación de los certificados, y siguiendo el estándar RFC 5280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"), los certificados emitidos a partir del 17 de abril de 2008 emplean la codificación UTF8String para los campos que contengan caracteres especiales, y PrintableString para el resto.

En los certificados emitidos con anterioridad a dicha fecha, los campos con caracteres especiales empleaban la codificación PrintableString, extendida de manera no estándar para interpretar caracteres especiales (como acentos o la "ñ") según la codificación Latin-1.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

El OID de la CPS es el siguiente: 1.3.6.1.4.1.13177.10.0.V, donde V indica la versión del documento.

Los OID de cada certificado incluido en las políticas de certificación de cada tipo de certificado se encuentran detallados en el primer capítulo del presente documento.

7.1.7 Extensión del uso de las restricciones de política

Sin estipulación.

7.1.8 Sintaxis y semántica de los "PolicyQualifier"

Se utilizan dos PolicyQualifiers en la extensión Certificate Policies:

- id-qt-cps: Contiene la URL donde se puede encontrar la CPS y las CP.
- id-qt-unotice: Nota de texto que se puede desplegar en la pantalla del usuario durante la verificación del certificado.

7.1.9 Tratamiento semántico para la extensión "Certificate Policy"

La extensión Certificate Policy permite identificar la política que Firmaprofesional asocia al certificado y dónde se pueden encontrar dichas políticas.

Está compuesta por 3 elementos: el OID de la política y los dos PolicyQualifiers definidos anteriormente.

7.2 Perfil de CRL

El perfil de las CRL's se corresponde con el propuesto en las políticas de certificación correspondientes, y con el estándar X.509 versión 3 de la RFC 5280 "Internet X.509 Public Key

Infrastructure Certificate and CRL Profile". Las CRL's son firmadas por la autoridad de certificación que ha emitido los certificados.

7.2.1 Número de versión

Las CRL emitidas por la CA son de la versión 2.

7.2.2 CRL y extensiones

7.2.2.1 CRL de la autoridad raíz

Campos	**Valores**
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha2WithRSAEncryption (para la CA Root "Autoridad de Certificacion Firmaprofesional CIF A62634068") ecdsa-with-SHA384 (para el resto de CAs Roots)
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
Fecha de próxima actualización	Fecha efectiva de emisión + 6 meses
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

7.2.2.2 CRL de las autoridades de certificación subordinadas

Campos	Valores
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha2WithRSAEncryption o ecdsa-with-SHA384 en función de las subordinadas.
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
fecha de próxima actualización	Fecha efectiva de emisión + 7 días
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

7.3 Perfil de OCSP

El perfil de OCSP viene especificado en el apartado 5 del documento "Perfiles de Certificados".

7.3.1 Número de versión

Los servicios de OCSP cumplen con la norma IETF RFC 6960.

7.3.2 OCSP y extensiones

Sin estipulación.

El certificado OCSP no empleará la extensión AIA "id-ad-ocsp" accessMethod

8 Auditorías de cumplimiento y otros controles

8.1 Frecuencia de las auditorías

Se realizan auditorías periódicas, generalmente con carácter anual.

8.2 Cualificación del auditor

Las auditorías pueden ser de carácter tanto interno como externo. En este segundo caso se realizan por empresas de reconocido prestigio en el ámbito de las auditorías.

Para el caso de auditorías externas de cumplimiento de eIDAS, Firmaprofesional las realizará con un CAB (Conformity Assessment Body).

Para las auditorías de cumplimiento de los requisitos del CA/Browser Forum, Firmaprofesional las realizará con una organización aceptada por la Fundación Mozilla para tal fin.

Firmaprofesional podrá establecer otros criterios de auditoría, de entre otros posibles aceptados comúnmente en el mercado para la actividad de la CA, o por el establecimiento de criterios por la normativa vigente.

El auditor deberá tener una cualificación y formación acorde a la auditoría que va a realizar.

8.3 Relación entre el auditor y la autoridad auditada

Las empresas que realizan las auditorías externas nunca representan ningún conflicto de intereses que pueda desvirtuar su actuación en su relación con Firmaprofesional.

No obstante, Firmaprofesional realiza auditorías periódicas internas a las CA de la jerarquía para garantizar en todo momento su adecuación a los requerimientos marcados por las políticas de certificación de la jerarquía.

8.4 Aspectos cubiertos por los controles

La auditoría verifica los siguientes principios:

a. **Publicación de la Información.** Que la CA hace públicas las Prácticas de Negocio y de Gestión de Certificados (la presente CPS), así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en conformidad con dichas afirmaciones.

b. **Integridad de Servicio.** Que la CA mantiene controles efectivos para asegurar razonablemente que:

   - La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la CA), y

   - La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

c. **Controles generales.** Que la CA mantiene controles efectivos para asegurar razonablemente que:

   - La información de suscriptores y usuarios está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio de la CA publicadas.

   - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.

Las tareas de explotación, desarrollo y mantenimiento de los sistemas de la CA son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos.

8.4.1 Auditoría en las Autoridades de Registro

Las Autoridades de Registro que tengan acceso al software facilitado por Firmaprofesional para la gestión de certificados son auditadas previamente a su puesta en marcha efectiva.

Adicionalmente, se realizan auditorías que comprueban el cumplimiento de los requerimientos exigidos por las políticas de certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado. La periodicidad de las auditorías vendrá determinada por el acuerdo entre Firmaprofesional y la Autoridad de Registro, siempre teniendo en cuenta la actividad prevista a desarrollar por la Autoridad de Registro en cuanto a número de certificados o requerimientos específicos de seguridad.

No obstante, y excepcionalmente, Firmaprofesional podría eximir a una Autoridad de Registro de la obligación de someterse a una auditoría inicial y a las auditorías de mantenimiento.

8.5 Acciones a emprender como resultado de la detección de deficiencias

En caso de que sean detectadas incidencias o no-conformidades, se habilitarán las medidas oportunas para su resolución en el menor tiempo posible. Para no-conformidades graves (afectan a los servicios críticos, a saber, SERVICIOS DE REVOCACIÓN, SERVICIOS DE ACTIVACIÓN / SUSPENSIÓN DE CERTIFICADOS, SERVICIOS DE PUBLICACIÓN DE CRL), Firmaprofesional se compromete a su resolución en un plazo máximo de tres meses.

En todo caso se formará un comité de resolución formado por personal de las áreas afectadas y otro de seguimiento formado por los responsables de las áreas afectadas y Dirección General.

8.6 Comunicación de resultados

El auditor comunicará los resultados al director técnico y al Director General, en tanto que responsable máximo de Firmaprofesional.

9 Otras cuestiones legales y de actividad

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

Los precios de los servicios de certificación o cualquier otro servicio serán facilitados a los clientes o posibles clientes por el Departamento Comercial de Firmaprofesional

9.1.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos es gratuito. No obstante, la CA se reserva el derecho de imponer una tarifa en determinados casos como la descarga masiva de certificados o cualquier otra circunstancia que a juicio de la CA deba ser gravada.

9.1.3 Tarifas de acceso a la información de estado o revocación

Firmaprofesional provee un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito, por medio de la publicación de las correspondientes CRL y del servicio OCSP.

Firmaprofesional ofrece otros servicios de validación de certificados comerciales, cuyas tarifas serán negociadas con cada cliente de estos servicios.

9.1.4 Tarifas de otros servicios

Las tarifas aplicables a otros servicios se negociarán entre Firmaprofesional y los clientes de los servicios ofrecidos.

9.1.5 Política de reembolso

Sin estipulación.

9.2 Responsabilidades económicas

Firmaprofesional, en su actividad como Prestador de Servicios de Certificación dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad de PSC tal como se define en la legislación española vigente.

Dichas garantías no son aplicables a los certificados que no sean cualificados, por lo que la cuantía que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial se limita a un máximo de 6.000 €.

Firmaprofesional no responderá de los perjuicios que la pérdida de cualificación de los dispositivos cualificados de creación de firma (tarjeta, token o HSM) y la consecuente y obligada revocación de los certificados pudiese ocasionar al usuario o a terceros. El CLIENTE conoce y acepta que los dispositivos cualificados de creación de firma (tarjeta o token) no podrán ser reutilizados una vez que caduquen los certificados.

9.2.1 Cobertura de seguro

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura de 3.000.000 € o conforme a la normativa vigente a la legislación española para los prestadores de servicios de confianza y la cobertura exigida por las EV Guidelines del CA/Browser Forum.

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

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

Firmaprofesional cumple en todo caso con la normativa vigente en materia de protección de datos y concretamente con lo dispuesto por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

9.3.1 Ámbito de la información confidencial

Firmaprofesional considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

9.3.2 Información no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente CPS.
- La contenida en las distintas Políticas de Certificación (CP).
- La contenida en los distintos Textos de Divulgación (PDS).
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

9.3.3 Responsabilidad en la protección de información confidencial

Es responsabilidad de Firmaprofesional establecer medidas adecuadas para la protección de la información confidencial.

9.4 Protección de la información personal

9.4.1 Política de protección de datos de carácter personal

En cumplimiento de los requisitos establecidos en la normativa aplicable en materia de protección de datos de carácter personal, Firmaprofesional dispone de un Registro de Actividades de Tratamiento de datos de carácter personal, donde está recogido el fichero "BBDD CERTIFICADOS", cuya finalidad es la gestión de los certificados emitidos y la prestación de los servicios de certificación asociados.

9.4.1.1 Aspectos cubiertos

El presente documento describe los procedimientos, requisitos y obligaciones en relación a la obtención y gestión de los datos de carácter personal, cumpliendo con lo establecido en la vigente normativa de protección de datos de carácter personal y las medidas de seguridad aplicables.

9.4.2 Información tratada como privada

De conformidad con lo establecido en el artículo 4 del Reglamento general de protección de datos (RGPD), se consideran datos personales cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados en todo caso como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por la Autoridad de Certificación.
- Toda otra información identificada como privada.

En cualquier caso, los datos captados por el Prestador de Servicios de Certificación deberán ser tratados con el de nivel de seguridad adecuado al riesgo que presente cada tratamiento.

9.4.2.1 Estructura de los tratamientos de ficheros de carácter personal

Ámbito personal	Nombre y Apellidos
	E-mail
	Lugar y Fecha de nacimiento
	País
	Número del DNI
Ámbito profesional	CIF correspondiente a la persona o entidad a la que está vinculado el firmante
	Departamento o Unidad al que pertenezca el firmante
	Cargo, título o rol del firmante en la organización
	Ubicación geográfica del firmante en la organización (empresa o colegio)
	Número de empleado o colegiado profesional

9.4.3 Información no calificada como privada

La siguiente información no está calificada como privada:

- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.

- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.

9.4.4 Responsabilidad de la protección de los datos de carácter personal

La información confidencial de acuerdo con el RGPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en las medidas de seguridad aplicables por Firmaprofesional.

Ante cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes, Firmaprofesional notificará al supervisor nacional competente en materia de servicios electrónicos de confianza y a la Autoridad de protección de datos correspondiente, en un plazo de 24 horas tras tener conocimiento de los hechos de acuerdo con el artículo 19.2 del Reglamento eIDAS.

9.4.5 Comunicación y consentimiento para usar datos de carácter personal

La autorización del usuario para el tratamiento automatizado de los datos personales suministrados para la prestación de servicios pactados, así como para la oferta y contratación de otros productos y servicios de Firmaprofesional, S.A, será requerida mediante la firma y aceptación del instrumento jurídico vinculante.

La información obtenida es usada tanto para la correcta identificación de los usuarios que solicitan servicios personalizados, como para la realización de estudios estadísticos de los usuarios registrados que permitan diseñar mejoras en los servicios prestados, llevar a cabo tareas básicas de administración y poder comunicar incidencias, ofertas y novedades a los usuarios registrados vía correo electrónico.

La información personal recabada de los usuarios registrados es almacenada en la base de datos propiedad de Firmaprofesional que asume las medidas de índole técnica, organizativa y de seguridad para garantizar la confidencialidad e integridad de la información de acuerdo con lo establecido en el Reglamento General de Protección de Datos (RGPD), y la Ley Orgánica 3/2018 de protección de datos personales y garantía de los derechos digitales.

El usuario responderá, en cualquier caso, de la veracidad de los datos facilitados, reservándose Firmaprofesional el derecho a excluir de los servicios registrados a todo usuario que haya facilitado datos falsos, sin perjuicio de las demás acciones legales.

Cualquier usuario registrado puede en cualquier momento ejercer el derecho de acceso, rectificación, oposición, supresión, limitación al tratamiento y portabilidad de sus datos de carácter personal suministrados a Firmaprofesional mediante comunicación escrita con referencia "tratamiento de datos".

No obstante, si el usuario considera que su derecho a la protección de datos personales ha podido ser vulnerado, puede reclamar ante la Agencia Española de Protección de Datos.

9.4.6 Revelación en el marco de un proceso judicial

Los datos de carácter personal podrán ser revelados por Firmaprofesional sin el previo consentimiento del suscriptor en el marco de un proceso judicial, en cumplimiento de una obligación legal.

9.4.7 Otras circunstancias de publicación de información

Aquellas descritas en el punto 1 del artículo 6 del Reglamento General de Protección de Datos (RGPD).

9.5 Derechos de propiedad intelectual

a. Propiedad de la CPS

La propiedad intelectual de esta CPS y de las distintas CP pertenece a Firmaprofesional, S.A.

Firmaprofesional no cobra una tarifa por el acceso a esta CPS ni a las diferentes CP. Cualquier uso que se haga para fines distintos a la simple visualización de los documentos, como reproducción, redistribución, modificación o creación de un derivado de las mismas, estarán sujetas a un acuerdo de licencia con la entidad titular de los derechos de autor del documento.

b. Propiedad de los certificados

Firmaprofesional será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita si no se acuerda explícitamente lo contrario.

Firmaprofesional concede licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del

certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política y de acuerdo con el correspondiente instrumento vinculante entre Firmaprofesional y la parte que reproduzca y/o distribuya el certificado, así como con las correspondientes condiciones generales de emisión.

c. Propiedad de las claves

El par de claves es propiedad del suscriptor.

Las anteriores reglas figurarán en los instrumentos vinculantes entre las CAs y los suscriptores y los terceros que confían en certificados.

9.6 Obligaciones y garantías

9.6.1 Obligaciones de la CA

Firmaprofesional se obligan según lo dispuesto en este documento, así como lo dispuesto en la normativa sobre prestación de servicios de Certificación, la Ley 6/2020 y el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, principalmente a:

a. Respetar lo dispuesto en las Políticas y Prácticas de Certificación (la presente CPS, las CP y las PDS).

b. Publicar esta CPS, las CP y las PDS en su página Web.

c. Informar sobre las modificaciones de esta CPS a los suscriptores, a las RA que estén vinculadas a ella y usuarios, mediante la publicación de éstas y sus modificaciones en su página web.

d. Disponer de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.

e. Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad

Por lo que a certificados respecta:

a. Emitir certificados conforme a esta CPS y a los estándares de aplicación.

b. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.

c. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.

d. Publicar los certificados emitidos en un Registro de Certificados, únicamente si se dispone de la autorización del firmante y respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

e. Suspender y revocar los certificados según lo dispuesto en la CPS y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados) y en el servicio OCSP.

Sobre custodia de información:

a. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente, cuando sea aplicable.

b. No almacenar ni copiar los datos de creación de firma del Suscriptor, cuando así lo disponga la normativa vigente.

c. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia si así se contemplase.

d. Proteger sus claves privadas de forma segura.

e. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.

9.6.2 Obligaciones de la RA

Las Autoridades de Registro también se obliga en los términos definidos en la presente CPS para la emisión de certificados, principalmente a:

a. Respetar lo dispuesto en esta CPS y en la CP correspondiente al tipo de certificado que emita.

b. Respetar lo dispuesto en los contratos firmados con la CA.

c. Respetar lo dispuesto en los contratos firmados con el Suscriptor o firmante.

En el ciclo de vida de los certificados:

a. Comprobar la identidad de los solicitantes de certificados según lo descrito en esta CPS o mediante otro procedimiento que haya sido aprobado por Firmaprofesional.

b. Verificar la exactitud y autenticidad de la información suministrada por el suscriptor o solicitante.

c. Informar al solicitante, antes de la emisión de un certificado, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de Firmaprofesional, de la CPS, la PDS y de la CP correspondiente al certificado.

d. Tramitar y entregar los certificados conforme a lo estipulado en esta CPS, la PDS y en la CP correspondiente.

e. Formalizar el contrato de certificación con el suscriptor según lo establecido por la Política de Certificación aplicable.

f. Abonar las tarifas establecidas por los servicios de certificación solicitados.

g. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el suscriptor.

h. Informar a la CA las causas de revocación, siempre y cuando tomen conocimiento.

i. Realizar las comunicaciones con los suscriptores o firmantes, por los medios que consideren adecuados, para correcta gestión del ciclo de vida de los certificados. Concretamente realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las suspensiones, rehabilitaciones y revocaciones de los mismos.

j. Como Encargado del tratamiento de los datos personales por cuenta de la CA, la RA deberá cumplir con todas las obligaciones establecidas en el artículo 28 del Reglamento General de Protección de datos (RGPD)

9.6.3 Obligaciones de los solicitantes

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

a. Suministrar a la RA la información necesaria para realizar una correcta identificación.

b. Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.

c. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

d. Respetar lo dispuesto en los documentos contractuales firmados con la CA y la RA.

9.6.3.1 Obligaciones de los firmantes

El firmante estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a. Custodiar sus DCCF, claves privadas y códigos secretos de manera diligente.

b. Usar el certificado según lo establecido en la presente CPS.

c. Respetar lo dispuesto en los instrumentos jurídicos vinculantes con la CA y la RA.

d. Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión o revocación.

e. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

f. No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la CA o la RA de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.

9.6.4 Obligaciones de los terceros que confían en los certificados

Será obligación de los usuarios cumplir con lo dispuesto por la normativa vigente y además:

a. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

   En este sentido, los terceros que confíen, comprobarán que el certificado es cualificado consultando a la Lista de Confianza de la Unión Europea (TSL). La norma ETSI TS 119 615 proporciona orientación sobre cómo validar un certificado digital con las listas de confianza de la UE, con el fin de determinar si puede ser considerado como un certificado cualificado.

b. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

9.6.5 Obligaciones de otros participantes

Sin estipulación

9.7 Exención de garantía

Firmaprofesional puede rechazar toda garantía de servicio que no se encuentre vinculado a las obligaciones establecidas por la ley 6/2020, de 11 de noviembre y el Reglamento (UE) 910/2014 (eIDAS)

9.8 Responsabilidades

9.8.1 Responsabilidades de la Autoridad de Certificación

Firmaprofesional, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en las Políticas y Prácticas de certificación y allí donde sea aplicable, por lo que dispone la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento (UE) No 910/2014 (eIDAS).

Sin perjuicio de lo anterior Firmaprofesional no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la presente CPS, en la Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza , y en el Reglamento (UE) 910/2014 (eIDAS), donde sea aplicable.

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

- La exactitud de la información contenida en el certificado en la fecha de su emisión, siempre que ésta corresponda a información autenticada.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente aplicable.

9.8.2 Responsabilidades de la Autoridad de Registro

La RA asumirá toda la responsabilidad en el procedimiento de identificación de los suscriptores y en la verificación de la identidad. Deberá para ello proceder según lo estipulado en la presente CPS o según otro procedimiento aprobado por Firmaprofesional.

Si la generación del par de claves no se realiza en presencia del suscriptor, la RA será responsable de la custodia de las claves hasta su entrega al suscriptor.

9.8.3 Responsabilidades del suscriptor

Es responsabilidad del suscriptor cumplir con las obligaciones estipuladas en el presente documento y en la CP correspondiente, y en el instrumento jurídico vinculante.

9.8.4 Delimitación de responsabilidades

Firmaprofesional no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

a. Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor o por los Terceros, o cualquier otro caso de fuerza mayor.

b. Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.

c. Por el uso indebido de la información contenida en el Certificado o en la CRL.

d. Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.

e. En relación a acciones u omisiones del Solicitante y Suscriptor:

- Falta de veracidad de la información suministrada para emitir el certificado.
- Retraso en la comunicación de las causas de suspensión o revocación del certificado.
- Ausencia de solicitud de suspensión o revocación del certificado cuando proceda.
- Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Uso del certificado fuera de su periodo de vigencia, o cuando Firmaprofesional o la RA le notifique la revocación o suspensión del mismo.
- Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la presente CPS, en particular, superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por Firmaprofesional.

f. En relación a acciones u omisiones del tercero que confía en el certificado:

- Falta de comprobación de las restricciones que figuren en el certificado electrónico o en la presente CPS en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
- Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

9.9 Indemnizaciones

9.9.1 Alcance de la cobertura

El seguro se hará cargo de todas las cantidades que Firmaprofesional S.A. resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros.

9.9.2 Cobertura de seguro u otras garantías para los terceros aceptantes

No existe cobertura para los terceros aceptantes.

9.9.3 Limitaciones de pérdidas

Firmaprofesional limita su responsabilidad mediante la inclusión de los límites de uso del certificado, y límites del valor de las transacciones para las cuales pueden emplearse los mismos, expresadas en los propios certificados mediante la extensión qcStatements (OID 1.3.6.1.5.5.7.1.3) y en la CP correspondiente.

El suscriptor podrá, si lo desea, solicitar y en su caso contratar un límite superior al indicado, asumiendo los costes adicionales que en su caso se establezcan. Además, el suscriptor y terceras partes podrán acordar bilateralmente pactos o coberturas específicas para transacciones de valor superior, manteniéndose en este caso el límite de responsabilidad de la CA citado en los párrafos anteriores, según la política de certificación aplicable.

9.10 Periodo de validez

9.10.1 Plazo

La CPS, las PDS y las distintas CP entran en vigor en el momento de su publicación.

9.10.2 Sustitución y derogación de la CPS

La presente CPS, las PDS y las distintas CP serán derogadas 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 CPS o 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

Firmaprofesional establece en el instrumento jurídico vinculante con el suscriptor los medios y plazos para las notificaciones.

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

En caso de problemas de seguridad o de pérdida de integridad que puedan afectar a una persona física o jurídica, Firmaprofesional le notificará dicha incidencia sin ningún retraso.

Si Firmaprofesional fuera notificado sobre una dirección de correo electrónico por la que pueda contactar con la Autoridad Nacional Competente, deberá informar a dicha Autoridad Nacional Competente, a través de ese correo, sobre la forma que ésta puede autenticarse para realizar las solicitudes de revocación de los certificados emitidos en virtud de la Directiva de Servicios de Pago (UE) 2015/2366

9.12 Cambios en las especificaciones

9.12.1 Procedimiento para los cambios

9.12.1.1 Elementos que pueden cambiar sin necesidad de notificación

Los únicos cambios que pueden realizarse a esta política sin requerir de notificación son las correcciones tipográficas o de edición o los cambios en los detalles de contacto.

9.12.1.2 Cambios con notificación

Los elementos de esta CPS pueden ser cambiados unilateralmente por Firmaprofesional sin preaviso. Las modificaciones pueden traer causa justificativa en motivos legales, técnicos o comerciales.

Cuando corresponda, dichas modificaciones serán notificadas al Organismo de Supervisión correspondiente, y tras su aprobación definitiva, se publicará la nueva documentación con un periodo de entrada en vigor que posibilite la posible rescisión de los suscriptores que no acepten los cambios. El momento de entrada en vigor se anunciará suficientemente en el momento de publicación de los cambios.

9.12.1.3 Mecanismo de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los suscriptores, usuarios o terceros serán notificados inmediatamente a los interesados mediante la publicación en la Web de Firmaprofesional.

Las RA podrán ser notificadas directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

9.12.2 Periodo y procedimiento de notificación

Las personas, instituciones o entidades afectadas pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 45 días siguientes a la notificación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la organización responsable de la administración de las políticas.

9.12.3 Circunstancias en las que el OID debe ser cambiado

Se procederá al cambio de OID en aquellas circunstancias que se altere alguno de los procedimientos descritos en el presente documento o en alguna de las CP, y que afecte directamente al modo operativo de alguna de las entidades participantes.

9.13 Reclamaciones y resolución de conflictos

Para la resolución de cualquier conflicto que pudiera surgir en relación con este documento, las CP o el instrumento jurídico vinculante, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la Corte Española de Arbitraje.

9.14 Normativa aplicable

La normativa aplicable al presente documento, así como a las distintas CP, y a las operaciones que derivan de ellas, es la siguiente:

- Reglamento (UE) No 910/2014 del parlamento europeo 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 y por la que se deroga la Directiva 1999/93/CE
- Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales(LO 3/2018)

- Directiva (UE) 2015/2366 del 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.

- Reglamento de Ejecución (UE) 2015/1502 DE LA COMISIÓN de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

- Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

- Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguro.

- Última versión de los "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" publicados en http://www.cabforum.org por el CA/Browser Forum. En caso de cualquier inconsistencia entre esta Declaración de Prácticas de Certificación y los citados requisitos, prevalecerán dichos requisitos.

- Guidelines For The Issuance And Management Of Extended Validation Certificates, publicados en http://www.cabforum.org por el CA/Browser Forum. En caso de cualquier inconsistencia entre este documento y esas Directrices, esas Directrices prevalecen sobre este documento.

9.15 Cumplimiento de la normativa aplicable

Firmaprofesional manifiesta el cumplimiento de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el Reglamento (UE) 910/2014 (eIDAS) así como de la normativa relacionada en el punto anterior.

Si se produjera alguna inconsistencia entre la ley nacional aplicable y los Baseline Requirements o EV SSL Certificate Guidelines, la CPS puede ajustarse para satisfacer los requisitos de dichas leyes nacionales. Sin embargo, el CA/Browser Forum será notificado inmediatamente de cualquier ajuste de este tipo.

9.16 Estipulaciones diversas

9.16.1 Cláusula de aceptación completa

Todos los terceros que confían en los certificados asumen en su totalidad el contenido de la última versión de este documento, las PDS y de las CP correspondientes.

9.16.2 Independencia

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

9.16.3 Resolución por la vía judicial

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

9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)

Sin estipulación.

9.16.5 Fuerza mayor

Firmaprofesional no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de guerra, desastres naturales,
- funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Cliente o por los Terceros, o
- cualquier otro caso de fuerza mayor.

9.17 Otras provisiones

Sin estipulación.