DECLARACION DE PRÁCTICAS DE CERTIFICACION (CPS) DE FIRMAPROFESIONAL, S.A.

Declaración de Prácticas de Certificación

Versión: 151005
Clasificación: Público

ATENCIÓN: El original vigente de este documento se encuentra en formato electrónico en la web de Firmaprofesional: https://www.firmaprofesional.com/cps

Histórico de versiones

Versión	Sección y cambios
6.1	*(para consultar cambios entre versiones anteriores, por favor envíe un correo a info@firmaprofesional.com)*

151005	<u>Sección "1.3.2 Autoridad de Certificación (CA)":</u>
	• 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
	<u>Sección "1.4.3 Certificados para la Administración Pública":</u>
	• Se elimina el certificado de Sede Electrónica, que se traslada a la sección "Certificados de Servicio Seguro", por coherencia funcional.
	<u>Sección "2.1 Repositorios":</u>
	• Se actualiza la tabla
	<u>Sección "5.8.2 Autoridad de Registro":</u>
	• Se añade la obligación a la RA de entregar toda la documentación a Firmaprofesional.
	<u>Sección "6.1.5 Tamaño de las claves":</u>
	• Dada la diversidad de políticas de certificado se abre la definición del período de validez para los certificados de entidad final

Índice

1 INTRODUCCIÓN 11
1.1 Presentación 11
1.2 Nombre del documento 12
1.2.1 Identificación 12
1.2.2 OIDs 12
1.3 Entidades participantes 13
1.3.1 Prestador de Servicios de Certificación (PSC) 13
1.3.2 Autoridad de Certificación (CA) 13
1.3.3 Autoridad de Registro (RA) 22
1.3.4 Solicitante 23
1.3.5 Suscriptor 23
1.3.6 Firmante 23
1.3.7 Tercero que confía en los certificados 23
1.4 Tipos de certificados 24
1.4.1 Certificados Corporativos Reconocidos 24
1.4.2 Certificados Corporativos de uso restringido 24
1.4.3 Certificados para la Administración Pública 25
1.4.4 Certificados Personales Reconocidos 26
1.4.5 Certificados de Servicio Seguro 26
1.4.6 Certificados de Firma Electrónica Avanzada 27
1.5 Usos no autorizados de los certificados 27
1.6 Administración de las políticas 28
1.6.1 Organización responsable 28
1.6.2 Persona de contacto 28
1.6.3 Frecuencia de revisión 28
1.6.4 Procedimiento de aprobación 28
1.7 Definiciones y acrónimos 28
1.7.1 Definiciones 28
1.7.2 Acrónimos 30
2 REPOSITORIOS Y PUBLICACION DE INFORMACION 32
2.1 Repositorios 32
2.2 Publicación de información 33
2.2.1 Políticas y Prácticas de Certificación 33
2.2.2 Términos y condiciones 33

2.2.3 Difusión de los certificados 33
2.3 Frecuencia de publicación 33
2.4 Control de acceso a los repositorios 33
3 IDENTIFICACIÓN Y AUTENTICACIÓN 35
3.1 Registro de Nombres 35
3.1.1 Tipos de nombres 35
3.1.2 Necesidad de que los nombres sean significativos 35
3.1.3 Uso de seudónimos 35
3.1.4 Reglas para interpretar varios formatos de nombres 35
3.1.5 Unicidad de los nombres 35
3.1.6 Reconocimiento, autenticación y papel de las marcas registradas 36
3.2 Validación inicial de la identidad 36
3.2.1 Método de prueba de posesión de la clave privada 36
3.2.2 Autenticación de la identidad de una persona jurídica 36
3.2.3 Autenticación de la identidad de una persona física 36
3.2.4 Autenticación de la identidad de la RA y de operadores de RA 37
3.2.5 Validación del dominio 38
3.2.6 Validación del correo electrónico 38
3.3 Identificación y autenticación en la renovación de certificados 38
3.3.1 Renovación de certificados online 38
3.3.2 Renovación presencial de certificados 39
3.4 Identificación y autenticación en la revocación de certificados 39
4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 40
4.1 Solicitud de certificados 40
4.1.1 Quién puede solicitar un certificado 40
4.1.2 Procesos de solicitud de certificados 40
4.2 Tramitación de las solicitudes de certificados 41
4.2.1 Realización de las funciones de identificación y autenticación 41
4.2.2 Aprobación o denegación de las solicitudes de certificados 41
4.3 Emisión de certificados 41
4.3.1 Acciones de la CA durante la emisión de los certificados 41
4.3.2 Notificación al Subscriptor por la CA de la emisión del certificado 42
4.4 Aceptación del certificado 42
4.4.1 Forma en la que se acepta el certificado 42
4.4.2 Publicación del certificado 42
4.5 Uso de las claves y el certificado 42

4.5.1 Uso de la clave privada y del certificado por el suscriptor 42
4.5.2 Uso de la clave pública y del certificado por los terceros que confían en los certificados 43
4.6 Renovación de certificados sin cambio de claves 43
4.7 Renovación con cambio de claves 43
4.7.1 Circunstancias para la renovación online 43
4.7.2 Quién puede pedir la renovación online de un certificado 43
4.7.3 Solicitud de renovación online 43
4.7.4 Tramitación de las peticiones de renovación online 44
4.7.5 Notificación de la emisión del certificado renovado 44
4.7.6 Forma de aceptación del certificado renovado 44
4.7.7 Publicación del certificado renovado 44
4.8 Modificación de certificados 44
4.9 Revocación y suspensión de certificados 45
4.9.1 Causas para la revocación 45
4.9.2 Quién puede solicitar la revocación 46
4.9.3 Procedimientos de solicitud de revocación 47
4.9.4 Plazo en el que la CA debe resolver la solicitud de revocación 48
4.9.5 Obligación de verificación de las revocaciones por los terceros 48
4.9.6 Frecuencia de emisión de CRLs 48
4.9.7 Tiempo máximo entre la generación y la publicación de las CRL 48
4.9.8 Disponibilidad del sistema en línea de verificación del estado de los certificados 48
4.9.9 Requisitos de comprobación de revocación en línea 49
4.9.10 Circunstancias para la suspensión 49
4.9.11 Quién puede solicitar la suspensión 49
4.9.12 Límites del periodo de suspensión 49
4.10 Servicios de información del estado de certificados 50
4.10.1 Características operativas 50
4.10.2 Disponibilidad del servicio 50
4.10.3 Características adicionales 50
4.11 Finalización de la suscripción 50
4.12 Custodia y recuperación de claves 50
5 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES 51
5.1 Controles físicos 51
5.1.1 Ubicación física y construcción 51
5.1.2 Acceso físico 52

5.1.3 Alimentación eléctrica y aire acondicionado 52
5.1.4 Exposición al agua 52
5.1.5 Protección y prevención de incendios 52
5.1.6 Sistema de almacenamiento 52
5.1.7 Eliminación de los soportes de información 53
5.1.8 Copias de seguridad fuera de las instalaciones 53
5.2 Controles de procedimiento 53
5.2.1 Roles de los responsables 53
5.2.2 Número de personas requeridas por tarea 54
5.2.3 Identificación y autenticación por rol 54
5.2.4 Roles que requieren segregación de funciones 54
5.3 Controles de personal 55
5.3.1 Requisitos relativos a la calificación, conocimiento y experiencia profesionales 55
5.3.2 Procedimientos de comprobación de antecedentes 55
5.3.3 Requerimientos de formación 55
5.3.4 Requerimientos y frecuencia de actualización de la formación 55
5.3.5 Sanciones por actuaciones no autorizadas 56
5.3.6 Requisitos de contratación de terceros 56
5.3.7 Documentación proporcionada al personal 56
5.4 Procedimientos de auditoría de seguridad 56
5.4.1 Tipos de eventos registrados 56
5.4.2 Frecuencia de procesado de registros de auditoría 57
5.4.3 Periodo de conservación de los registros de auditoría 57
5.4.4 Protección de los registros de auditoría 58
5.4.5 Procedimientos de respaldo de los registros de auditoría 58
5.4.6 Sistema de recogida de información de auditoría 58
5.4.7 Análisis de vulnerabilidades 58
5.5 Archivo de registros 58
5.5.1 Tipo de eventos archivados 58
5.5.2 Periodo de conservación de registros 59
5.5.3 Protección del archivo 59
5.5.4 Procedimientos de copia de seguridad del archivo 59
5.5.5 Requerimientos para el sellado de tiempo de los registros 59
5.5.6 Sistema de archivo de información de auditoría 60
5.5.7 Procedimientos para obtener y verificar información archivada 60
5.6 Cambio de claves de la CA 60
5.6.1 CA Raíz 60

5.6.2 CA Subordinada....60
5.7 Plan de recuperación de desastres....60
5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades....60
5.7.2 Alteración de los recursos hardware, software y/o datos....61
5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una Autoridad de Certificación....61
5.7.4 Continuidad del Negocio después de un desastre....61
5.8 Cese de actividad....61
5.8.1 Autoridad de Certificación....61
5.8.2 Autoridad de Registro....62
6 CONTROLES DE SEGURIDAD TÉCNICA....63
6.1 Generación e instalación del par de claves....63
6.1.1 Generación del par de claves....63
6.1.2 Entrega de la clave privada al firmante....63
6.1.3 Entrega de la clave pública al emisor del certificado....63
6.1.4 Entrega de la clave pública de la CA a los terceros que confían en los certificados 63
6.1.5 Tamaño de las claves....64
6.1.6 Parámetros de generación de la clave pública y verificación de la calidad....64
6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509v3)....64
6.2 Protección de la clave privada y controles de ingenieria de los módulos criptográficos....64
6.2.1 Estándares para los módulos criptográficos....64
6.2.2 Control multipersona (k de n) de la clave privada....65
6.2.3 Custodia de la clave privada....65
6.2.4 Copia de seguridad de la clave privada....65
6.2.5 Archivo de la clave privada....65
6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico....66
6.2.7 Método de activación de la clave privada....66
6.2.8 Método de desactivación de la clave privada....66
6.2.9 Método de destrucción de la clave privada....66
6.3 Otros aspectos de la gestión del par de claves....66
6.3.1 Archivo de la clave pública....66
6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves.66
6.4 Datos de activación....67
6.4.1 Generación e instalación de los datos de activación....67
6.4.2 Protección de los datos de activación....67

6.5 Controles de seguridad informática 67
6.5.1 Requerimientos técnicos de seguridad específicos 68
6.5.2 Evaluación de la seguridad informática 68
6.6 Controles de seguridad del ciclo de vida 68
6.6.1 Controles de desarrollo de sistemas 68
6.6.2 Controles de gestión de seguridad 69
6.7 Controles de seguridad de la red 72
6.8 Fuente de tiempo 72
7 PERFILES DE LOS CERTIFICADOS, CRL Y OCSP 73
7.1 Perfil de los certificados 73
7.1.1 Número de versión 73
7.1.2 Extensiones de los certificados 73
7.1.3 Identificadores de objeto (OID) de los algoritmos utilizados 74
7.1.4 Formatos de nombres 74
7.1.5 Restricciones de los nombres 75
7.1.6 Identificador de objeto (OID) de la Política de Certificación 75
7.1.7 Sintaxis y semántica de los “PolicyQualifier” 75
7.1.8 Tratamiento semántico para la extensión “Certificate Policy” 76
7.2 Perfil de CRL 76
7.2.1 Número de versión 76
7.2.2 CRL y extensiones 76
7.3 Perfil de OCSP 77
8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES 78
8.1 Frecuencia de las auditorias 78
8.2 Cualificación del auditor 78
8.3 Relación entre el auditor y la autoridad auditada 78
8.4 Aspectos cubiertos por los controles 79
8.4.1 Auditoría en las Autoridades de Registro 79
8.5 Acciones a emprender como resultado de la detección de incidencias 80
8.6 Comunicación de resultados 80
9 OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD 81
9.1 Tarifas 81
9.1.1 Tarifas de emisión de certificado o renovación 81
9.1.2 Tarifas de acceso a los certificados 81

9.1.3 Tarifas de acceso a la información de estado o revocación 81
9.1.4 Tarifas de otros servicios 81
9.2 Responsabilidades económicas 81
9.3 Confidencialidad de la información 82
9.3.1 Ámbito de la información confidencial 82
9.3.2 Información no confidencial 82
9.3.3 Responsabilidad en la protección de información confidencial 82
9.4 Protección de la información personal 83
9.4.1 Política de protección de datos de carácter personal 83
9.4.2 Información tratada como privada 84
9.4.3 Información no calificada como privada 85
9.4.4 Responsabilidad de la protección de los datos de carácter personal 85
9.4.5 Comunicación y consentimiento para usar datos de carácter personal 85
9.4.6 Revelación en el marco de un proceso judicial 86
9.4.7 Otras circunstancias de publicación de información 86
9.5 Derechos de propiedad intelectual 86
9.6 Obligaciones 87
9.6.1 Obligaciones de la CA 87
9.6.2 Obligaciones de la RA 88
9.6.3 Obligaciones de los solicitantes 89
9.6.4 Obligaciones de los firmantes 89
9.6.5 Obligaciones de los terceros que confían en los certificados 90
9.7 Exención de garantía 90
9.8 Responsabilidades 90
9.8.1 Responsabilidades de la Autoridad de Certificación 90
9.8.2 Responsabilidades de la Autoridad de Registro 91
9.8.3 Responsabilidades del suscriptor 91
9.8.4 Delimitación de responsabilidades 91
9.9 Indemnizaciones 92
9.9.1 Alcance de la cobertura 92
9.9.2 Cobertura de seguro u otras garantías para los terceros aceptantes 92
9.9.3 Limitaciones de pérdidas 92
9.10 Periodo de validez 93
9.10.1 Plazo 93
9.10.2 Sustitución y derogación de la CPS 93
9.10.3 Efectos de la finalización 93
9.11 Notificaciones individuales y comunicación con los participantes 93

9.12 Cambios en las especificaciones 93
9.12.1 Procedimiento para los cambios 93
9.12.2 Periodo y procedimiento de notificación 94
9.12.3 Circunstancias en las que el OID debe ser cambiado 94
9.13 Reclamaciones y resolución de conflictos 94
9.14 Normativa aplicable 94
9.15 Cumplimiento de la normativa aplicable 95
9.16 Estipulaciones diversas 95
9.16.1 Cláusula de aceptación completa 95
9.16.2 Independencia 95
9.16.3 Resolución por la vía judicial 95

1 INTRODUCCIÓN

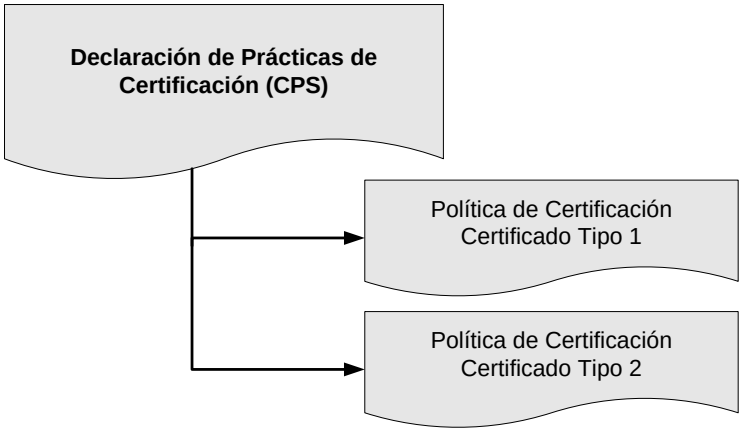
1.1 Presentación

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 reconocidos según la Ley 59/2003, de 19 de diciembre, de firma electrónica.

La **Ley 59/2003, de 19 de diciembre, de firma electrónica** 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 las Condiciones Generales establecidas en esta CPS, cada tipo de certificado emitido por Firmaprofesional se rige por unas condiciones particulares de emisión recogidas en un documento denominado "**Política de Certificación"** (en inglés CP o *Certificate Policy*). Existe una política de certificación por cada tipo de certificado emitido.



1.2 Nombre del documento

1.2.1 Identificación

Nombre:	Declaración de Practicas de Certificación (CPS)
Versión:	151005
Descripción:	Declaración de Prácticas de Certificación de Firmaprofesional S.A.
Fecha de Emisión:	15/10/2015
OID	1.3.6.1.4.1.13177.10.0.6.2
Localización	http://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.V.R	Declaración de Prácticas de Certificación (CPS)	V = Versión de la CPS R = Subversión de la CPS
10.1.T.D	Políticas de Certificación	T = Tipo de Certificado 1 = Corporativo de Colegiado 2 = Corporativo de Persona Física 3 = Servidor Web SSL 4 = Servicio Seguro (VA/TSA) 5 = Corporativo de Persona Jurídica 6 = Corporativo de Factura Electrónica 8 = Firma de Código 10= Corporativo de Sello Empresarial 11= Corporativo de Representante Legal 20= Sede Electrónica 21= Sello de Órgano 22= Empleado Público 30=Certificado de Infraestructura 40=Certificado Personal D = Dispositivo / Nivel de Seguridad 1 = DSCF (Nivel Alto) 2 = Otros dispositivos (Nivel Medio)
10.10.1	Política de Certificación de CA Subordinada	CA Subordinada
20.0.1	Política de Sellado de Tiempo	TSA Firmaprofesional

1.3 Entidades participantes

1.3.1 Prestador de Servicios de Certificación (PSC)

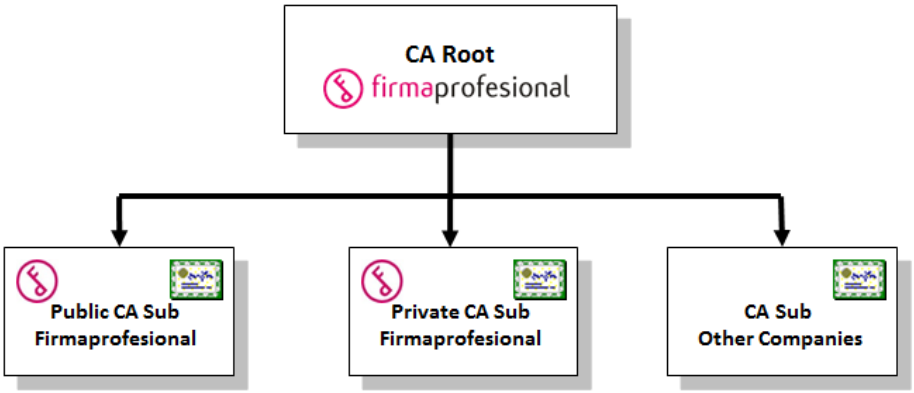
Firmaprofesional es un Prestador de Servicios de Certificación (PSC) que emite certificados reconocidos según la Ley de Firma Electrónica.

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 otras entidades por delegación soportada contractualmente con Firmaprofesional, que actuarán como intermediarios.

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

1.3.2 Autoridad de Certificación (CA)

El sistema de certificación de Firmaprofesional está 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.



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.

1.3.2.1 Autoridad de Certificación 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.

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.

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*
- *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*
- *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. Se recomienda que progresivamente, en la medida que las herramientas informáticas lo permitan, se vaya sustituyendo la CA Raíz SHA1 por la nueva CA Raíz SHA256

1.3.2.2 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 Industria, Energía y Turismo -MINETUR-), reconocidos por distintas plataformas (ej, Microsoft, Firefox, Chrome, Apple, Adobe, @Firma, PSIS o AEAT) y auditados por distintas normas (ej. Webtrust).

La Autoridad de Certificación Subordinada "***AC Firmaprofesional - CA1***" emite certificados digitales a Corporaciones Privadas, conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica:

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

La Autoridad de Certificación Subordinada "***AC Firmaprofesional - AAPP***" emite certificados digitales a Corporaciones Públicas, conforme a lo establecido en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos:

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

La Autoridad de Certificación Subordinada ***"AC Firmaprofesional - CUALIFICADOS***" emite certificados digitales reconocidos (cualificados) conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

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:

- ***CN = AC Firmaprofesional - CUALIFICADOS***
- *Hash SHA1: 3486 ED23 6221 5545 9E9B 25FF 3F21 AD76 2798 7387*
- *Válido desde el 18 de Septiembre de 2.014 hasta el 31 de Diciembre de 2.030*
- *Tipo de clave: RSA 2048 bits – SHA-256*

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 y SSL EV 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 o SSL EV.

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. 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*[1] y *Mozilla CA Certificate Inclusion Policy*[2].

- ***CN = AC Firmaprofesional – INFRAESTRUCTURA***
- *Hash SHA1: d52f 537f 62ce 24d0 6fb5 9b0a 02bf c4a8 f7c1 6b66*
- *Válido desde el 18 de Junio de 2013 hasta el 31 de Diciembre de 2030*
- *Tipo de Clave: RSA 2048 bits – SHA1*

- ***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*
- *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)*

1.3.2.3 Autoridades de Certificación Subordinadas Privadas

Las Autoridades de Certificación Subordinadas Privadas emiten certificados para uso privado entre entidades. 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

[1] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[2] Mozilla CA Certificate Inclusion Policy. Version 2.2

certificados públicos, ya que están operados desde la misma infraestructura y desde las mismas instalaciones.

La Autoridad de Certificación Subordinada "***AC Firmaprofesional - CFEA***" emite certificados digitales no reconocidos para servicios de firma electrónica avanzada.

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. 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*[3] y *Mozilla CA Certificate Inclusion Policy*[4].

- ***CN = AC Firmaprofesional - CFEA***
- *Hash SHA1: 6B66 7859 C1D8 C0F6 2F20 5B21 53D3 255C 7E16 CE0B*
- *Válido desde el 20 de Febrero de 2013 hasta el 31 de Diciembre de 2030*
- *Tipo de Clave: RSA 2048 bits – SHA1*

- ***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*
- *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)*

La Autoridad de Certificación Subordinada ***"AC Firmaprofesional – OTC"*** *(OTC: one-time certifícate)* emite certificados digitales no reconocidos para servicios de firma electrónica avanzada. Estos certificados tendrán una vigencia muy corta y estarán limitados para la firma de un único documento.

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. Ésta segunda está restringida técnicamente mediante el uso de la extensión *Extended Key Usage* (EKU – *extKeyUsage*) según lo establecido en los *Baseline Requirements*

[3] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[4] Mozilla CA Certificate Inclusion Policy. Version 2.2

Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[5] y *Mozilla CA Certificate Inclusion Policy*[6].

- ***CN = AC Firmaprofesional - OTC***
- *Hash SHA1: 1302 2ECD E763 0FB9 A14A 403E 74B0 FA3F A2A7 BCDA*
- *Válido desde el 20 de Febrero de 2013 hasta el 31 de Diciembre de 2030*
- *Tipo de Clave: RSA 2048 bits – SHA1*

- ***CN = AC Firmaprofesional - OTC***
- *Hash SHA1: 6e 13 b5 1c 6d 54 08 88 b8 ec c2 36 79 e9 1d 99 af f6 01 0d*
- *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)*

1.3.2.4 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 Certificación 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 Certificación.

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 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. Ésta segunda está restringida técnicamente mediante el uso de la extensión *Extended Key Usage* (EKU – *extKeyUsage*) según lo establecido en los *Baseline Requirements*

[5] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[6] Mozilla CA Certificate Inclusion Policy. Version 2.2

Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates[7] y *Mozilla CA Certificate Inclusion Policy*[8].

- ***CN=SIGNE Autoridad de Certificacion***
- *Hash SHA1: d730 47f2 cce5 64ef b0bc 8568 93ea 19d7 7469 398c*
- *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*

- ***CN=SIGNE Autoridad de Certificacion***
- *Hash SHA1: e6 b5 2b 5d 52 e5 cd e9 86 2a c1 de 66 8e c9 53 ad 36 59 bd*
- *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*

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, 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. 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*[9] y *Mozilla CA Certificate Inclusion Policy*[10].

- ***CN=SEU Autoridad de Certificacion***
- *Hash SHA1: 432C 2A08 ED3E 4ACB 87E8 4704 DCFD 9C3B D84D 18B7*
- *Válido desde el 20 de Febrero de 2.013 hasta el 31 de Diciembre de 2.030*
- *Tipo de clave: RSA 2048 bits – SHA1*
- *CPS: http://www.seu.com.co/dpc*

[7] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[8] Mozilla CA Certificate Inclusion Policy. Version 2.2
[9] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[10] Mozilla CA Certificate Inclusion Policy. Version 2.2

- ***CN=SEU Autoridad de Certificacion***
- *Hash SHA1: a9 e5 52 45 74 a8 ec 1f d3 16 18 54 c9 13 4c 47 97 de 7b 09*
- *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*

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, 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. 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*[11] y *Mozilla CA Certificate Inclusion Policy*[12].

- ***CN=Santander Digital Signature***
- *Hash SHA1: CF4E 801B 2774 B820 6A62 6371 AE32 37B7 C1D4 3F4E*
- *Hash MD5: 1CD9 FA19 8BEE A19E 8658 7D90 58BE 3E88*
- *Válido desde el 16 de Mayo de 2.012 hasta el 31 de Diciembre de 2.030*
- *Tipo de clave: RSA 2048 bits – SHA1*
- *CPS: http://www.tuisantander.com/cps*

[11] Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates. CA/Browser Forum. Version 1.3.0 April 16, 2015
[12] Mozilla CA Certificate Inclusion Policy. Version 2.2

- ***CN=Santander Digital Signature***
- *Hash SHA1: b0 0c 00 03 4b 72 3f 4d 95 37 35 3c 82 93 a9 45 51 4d ab 2d*
- *Válido desde el 29 de Julio de 2015 hasta el 31 de Diciembre de 2.030*
- *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*

1.3.2.5 Autoridades de Certificación Caducadas

El Certificado Raíz original de Firmaprofesional caducó el 25 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 MD5: 1192 7940 3CB1 8340 E5AB 664A 6792 80DF*
- *Válido desde el 25 de Octubre de 2001 al 25 de Octubre de 2013*
- *Longitud de clave RSA 2048 bits*

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***[13]". Gracias a ello los certificados de usuarios finales emitidos podían 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 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*

[13] La "Certificación Cruzada" es un mecanismo que permite crear caminos de certificación múltiples. En este caso sirve para que un mismo certificado se pueda validar indistintamente en dos jerarquías de certificación que acaban en CA Raíces distintas. (Ver "RFC4949: Internet Security Glossary, Version 2": cross-certification).

1.3.3 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.

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 otra 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 conocer y autorizar de manera expresa el acuerdo.

1.3.4 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.

1.3.5 Suscriptor

El Suscriptor es la persona física o jurídica que ha contratado los servicios de certificación de Firmaprofesional. Por lo tanto será el propietario del certificado.

En general, el suscriptor de un certificado de Firmaprofesional será una Corporación (empresa privada, entidad pública, colegio profesional), 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.

1.3.6 Firmante

El Firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona jurídica a la que representa.

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

1.3.7 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 reconocidos 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 reconocidos.

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 y en la Ley 59/2003 de

firma electrónica

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

1.4 Tipos de certificados

1.4.1 Certificados Corporativos Reconocidos

Los Certificados Corporativos Reconocidos son certificados reconocidos según la Ley 59/2003 de firma electrónica cuyo suscriptor es una Corporación (ya sea una empresa, una organización, un colegio profesional o una Administración Pública):

- **Certificados Corporativos de Colegiado**: Son certificados reconocidos de persona física que identifican al suscriptor como Colegio Profesional y al firmante como profesional colegiado por dicho Colegio.
- **Certificados Corporativos de Representante Legal:** Son certificados reconocidos de persona física que identifican al suscriptor como una Corporación y al firmante como representante legal de dicha Corporación.
- **Certificados Corporativos de Persona Jurídica**: Son certificados reconocidos de persona jurídica según el artículo 7 de la Ley 59/2003,
- **Certificados Corporativos de Persona Física**: Son certificados reconocidos de persona física que identifican al suscriptor como Corporación y al firmante como persona física vinculada a esa Corporación, ya sea como empleado, asociado, colaborador, cliente, proveedor u otro tipo de vinculación.

OID DE POLITICAS DE CERTIFICADOS	
1.3.6.1.4.1.13177.10.1.1.D	CP Corporativo de Colegiado
1.3.6.1.4.1.13177.10.1.2.D	CP Corporativo de Persona Física
1.3.6.1.4.1.13177.10.1.5.D	CP Corporativo de Persona Jurídica
1.3.6.1.4.1.13177.10.1.11.D	CP Corporativo de Representante Legal

D = Dispositivo / Nivel de Seguridad:
1 = DSCF (Nivel Alto), 2 = Otros dispositivos (Nivel Medio)

1.4.2 Certificados Corporativos de uso restringido

Los Certificados Corporativos de uso restringido son certificados electrónicos según la Ley 59/2003 de firma electrónica cuyo suscriptor es una Corporación (ya sea una empresa, una organización, un colegio profesional o una Administración Pública):

- **Certificados Corporativos de Factura Electrónica:** Son certificados reconocidos de persona física cuyo firmante está autorizado por la Corporación para firmar Facturas Electrónicas.

- **Certificados Corporativos de Sello Empresarial:** Son certificados electrónicos de persona jurídica limitados para determinados usos específicos.

  Los Certificados Corporativos de Sello Empresarial han sido autorizados para su utilización en facturación electrónica y digitalización certificada, mediante autorización expresa del Director del Departamento de Informática Tributaria, mecanismo que se recoge en el artículo 18 del Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido

OID DE POLITICAS DE CERTIFICADOS	
1.3.6.1.4.1.13177.10.1.10.D	CP Corporativo de Sello Empresarial
1.3.6.1.4.1.13177.10.1.6.D	CP Corporativo de Factura Electrónica

D = Dispositivo / Nivel de Seguridad:
1 = DSCF (Nivel Alto), 2 = Otros dispositivos (Nivel Medio)

1.4.3 Certificados para la Administración Pública

Los Certificados para la Administración Pública son certificados electrónicos emitidos según los requisitos establecidos en la **Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos**.

- **Certificado de Sello de Administración, Órgano o Entidad de Derecho Público:** Son certificados para dispositivos informáticos, programa o aplicaciones dedicados a firmar en nombre del órgano en sistemas de firma electrónica para la actuación administrativa automatizada.

- **Certificado de Empleado Público:** Son certificados reconocidos de persona física que identifican al suscriptor como Administración Pública y al firmante como empleado de la Administración.

OID DE POLITICAS DE CERTIFICADOS	
1.3.6.1.4.1.13177.10.1.21.D	CP Sello de Órgano
1.3.6.1.4.1.13177.10.1.22.D	CP Empleado Público

D = Dispositivo / Nivel de Seguridad:
1 = DSCF (Nivel Alto), 2 = Otros dispositivos (Nivel Medio)

1.4.4 Certificados Personales Reconocidos

Los Certificados Personales Reconocidos son certificados reconocidos según la Ley 59/2003 de firma electrónica:

- **Certificados Personales Reconocidos**: Son certificados reconocidos de persona física.

OID DE POLITICAS DE CERTIFICADOS	
1.3.6.1.4.1.13177.10.1.40.2	CP Personal

1.4.5 Certificados de Servicio Seguro

Firmaprofesional emite certificados digitales para usos diferentes a la firma electrónica reconocida. Estos certificados no están regulados por la Ley 59/2003. El suscriptor es una Corporación (ya sea una empresa, una organización, un colegio profesional o una Administración Pública):

- **Certificado de Servidor Web SSL:** Son certificados utilizados para autenticar un servidor Web por parte de los navegadores mediante el uso del protocolo HTTPS.
- **Certificado de Servidor Web SSL Extended Validation:** Son certificados utilizados para autenticar un servidor Web por parte de los navegadores mediante el uso del protocolo HTTPS con garantías extendidas de validación de la entidad propietaria del servidor.
- **Certificado de Sede Electrónica**: Son certificados expedidos a Administraciones Públicas para autenticar la identidad de la Sede Electrónica según los requisitos establecidos en la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- **Certificado de Firma de Código:** Son certificados utilizados para firmar código ejecutable, como por ejemplo un *applet* de Java, garantizando su autoría y su integridad frente a modificaciones no autorizadas.
- **Certificado de Infraestructura:** Son certificados utilizados para autenticar la identidad de un servidor mediante el uso de protocolos de comunicación cifrada como SAML, TLS o IPSEC.
- **Certificado de Servicio Seguro (VA/TSA):** Son certificados que permiten firmar evidencias digitales como Autoridad de Sellado de Tiempo (**TSA**) o Autoridad de Validación (**VA**). Su emisión y utilización requerirá las máximas garantías de seguridad.

OID DE POLITICAS DE CERTIFICADOS	
1.3.6.1.4.1.13177.10.1.3.1	CP de Servidor Web SSL
1.3.6.1.4.1.13177.10.1.3.10	CP de Servidor Web SSL EV
1.3.6.1.4.1.13177.10.1.20.1	CP Sede Electrónica
1.3.6.1.4.1.13177.10.1.30.1	CP de Infraestructura
1.3.6.1.4.1.13177.10.1.8.1	CP de Firma de Código
1.3.6.1.4.1.13177.10.1.4.1	CP de Servicio Seguro (TSA/VA)

1.4.6 Certificados de Firma Electrónica Avanzada

Los Certificados Privados son certificados firma electrónica avanzada no reconocidos según los términos de la Ley Firma Electrónica. Las características de estos certificados se definen para cada Suscriptor y son de uso privado para el entorno del Suscriptor.

Los certificados emitidos por Firmaprofesional cuya política no se mencione explícitamente en esta CPS o no dispongan de política específica publicada deben interpretarse como certificados de uso privado.

Estos certificados de uso privado no se emiten como reconocidos, por lo que no están sujetos a la obligación de disponer de unas políticas y prácticas de certificación publicadas, y su inclusión en la presente CPS es voluntaria.

1.5 Usos no autorizados 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 Practicas 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 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. 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 perdida de información derivada de la perdida de las claves de cifrado. Por ello, Firmaprofesional no recomienda el uso de los certificados digitales para el cifrado de la información.

1.6 Administración de las políticas

1.6.1 Organización responsable

El Departamento Técnico de Firmaprofesional es responsable de la administración de esta CPS y de las Políticas de Certificación.

1.6.2 Persona de contacto

Organización responsable:	Firmaprofesional, S.A.
Persona de contacto:	Director Técnico de Firmaprofesional
E-mail:	info@firmaprofesional.com
Teléfono:	+34 93 477 42 45
Dirección:	Firmaprofesional, S.A. Edificio ESADECREAPOLIS Avenida Torre Blanca, 57. Sant Cugat del Valles 08173 (Barcelona)

1.6.3 Frecuencia de revisión

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

1.6.4 Procedimiento de aprobación

La publicación de las revisiones de esta CPS y de las Políticas de Certificación 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.

1.7 Definiciones y acrónimos

1.7.1 Definiciones

- **Prestador de Servicios de Certificación:** persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- **Certificado Electrónico**: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un

firmante y confirma su identidad.

- **Certificado Reconocido**: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley 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 certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

- **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.

- **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 Seguro de Creación de Firma (DSCF)**: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica

- **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 Reconocida**: es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro 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**: 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.
- **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.

1.7.2 Acrónimos

CA: Autoridad de Certificación (Certification Authority)
CA Sub: Autoridad de Certificación Subordinada
CP: Política de Certificación (Certificate Policy)
CPS: Declaración de Prácticas de Certificación (Certificate Practice 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)
PKI: Infraestructura de Clave Públic (Public Key Infrastructure)
PSC: Prestador de Servicios de Certificación
RA: Autoridad de Registro (Registration Authority)
TSA: Autoridad de sellado de tiempo (Time Stamp Authority)
VA Autoridad de validación (Validation Authority)

<u>Estándares y Organismos de estandarización</u>

CEN: Comité Europeo de Normalización
CWA: CEN Workshop Agreement
ETSI: European Telecommunications Standard Institute
FIPS: Federal Information Processing Standard
IETF: Internet Engineer Task Force

PKIX: Grupo de trabajo del IETF sobre PKI

PKCS: Public Key Cryptography Standards

RFC: Request For Comments

2 REPOSITORIOS Y PUBLICACION DE INFORMACION

2.1 Repositorios

Acceso	Descripción	URL
Público	CPS y Políticas de Certificación	http://www.firmaprofesional.com/cps
Público	CA Raíz SHA1	http://crl.firmaprofesional.com/caroot.crt
Público	CA Raíz SHA256	http://crl.firmaprofesional.com/caroot256.crt
Público	CRL de CA Raíz	http://crl.firmaprofesional.com/fproot.crl
Público	CA Subordinada CA1	http://crl.firmaprofesional.com/ca1.crt
Público	CRL de CA Sub CA1	http://crl.firmaprofesional.com/firmaprofesional1.crl
Público	CA Subordinada AAPP	http://crl.firmaprofesional.com/fpaapp.crt
Público	CRL de CA Sub AAPP	http://crl.firmaprofesional.com/fpaapp.crl
Público	CA Subordinada CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crt
Público	CRL de CA Sub CUALIFICADOS	http://crl.firmaprofesional.com/cualificados.crl
Público	CA Sub INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crt
Público	CRL de CA Sub INFRAESTRUCTURA	http://crl.firmaprofesional.com/infraestructura.crl
Público	CA Subordinada CFEA	http://crl.firmaprofesional.com/cfea.crt
Público	CRL de CA Sub CFEA	http://crl.firmaprofesional.com/cfea.crl
Público	CA Subordinada CFEA	http://crl.firmaprofesional.com/otc.crt
Público	CRL de CA Sub CFEA	http://crl.firmaprofesional.com/otc.crl
Público	Servicio de Revocación	http://www.firmaprofesional.com
Restringido	Servicio de Sellado de Tiempo (TSA)	http://servicios.firmaprofesional.com/tsa
Restringido	Servicio de Validación (OCSP)	http://servicios.firmaprofesional.com/ocsp
Público	Servicio de Validación (OCSP)	http://ocsp.firmaprofesional.com

Los repositorios de Firmaprofesional están referenciados por la URL. Cualquier cambio en las URLs se notificará a todas 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

Tanto la CPS actual como las Políticas de Certificación de cada tipo de certificado estarán disponibles en formato electrónico en la Web de Firmaprofesional.

Las 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 Certificación*** y la aceptación de las ***Condiciones Generales de Contratación*** de Firmaprofesional publicadas en su web http://www.firmaprofesional.com/cps

2.2.3 Difusión de los certificados

El Suscriptor del certificado 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.

Firmaprofesional no está obligada a publicar los certificados emitidos en un repositorio de acceso público. Sin embargo, con el fin de mejorar los servicios a los clientes, Firmaprofesional podría ofrecer servicios de Directorio y de búsqueda y descarga de algunos certificados emitidos bajo su jerarquía de certificación.

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 Condiciones Generales de Contratación, los

certificados de CA y las listas de certificados revocados (CRL) se publicarán en repositorios de acceso público sin control de acceso.

Los certificados emitidos podrán publicarse en repositorios públicos o de acceso restringido según las necesidades. Los servicios de validación por el protocolo OCSP y 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 reconocidos son coherentes con lo dispuesto en las normas:

- ETSI TS 101 862 conocida como “European profile for Qualified Certificates”
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile",
- RFC 3739 “Qualified Certificates Profile”.

3.1.2 Necesidad de que los nombres sean significativos

Los campos del DN referentes al Nombre y Apellidos 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 reconocido en derecho.

En el caso que los datos consignados en el DN fueran ficticios o se indique expresamente su invalidez (ej. “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad.

3.1.3 Uso de seudónimos

Los certificados no admiten el uso de seudónimo de firmante en ningún caso.

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.

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. Sin embargo la CA no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.2 Validación inicial de la identidad

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

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.

3.2.3 Autenticación de la identidad de una persona física

La RA verificará de forma fehaciente 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.

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.

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 en certificados emitidos con posterioridad a la entrada en vigor de la Ley 59/2003, de 19 de diciembre, de firma electrónica, 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 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 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.

3.2.5 Validación del dominio

Para garantizar que una entidad solicitante tiene control sobre el dominio (URL) que solicita incluir en un certificado se realizan dos tipos de comprobaciones:

- **Organizacionales**: se solicita la titularidad del nombre de dominio, certificada por un representante legal de la organización.
- **Técnicas**: se consultan los siguientes servicios whois autenticados:
  - Para dominios "*.es": https://www.nic.es/sgnd/dominio/publicInformacionDominios.action
  - Para el resto de dominios: https://www.networksolutions.com/whois/index.jsp

3.2.6 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.

3.3 Identificación y autenticación en la renovación de certificados

3.3.1 Renovación de certificados online

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

- La RA ha autorizado la renovación.
- El certificado que desea renovar no ha caducado.

- En el caso de certificados reconocidos, han transcurrido menos de 5 años desde su última personación e identificación ante la RA[14].

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

3.3.2 Renovación presencial de certificados

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.

[14]Según el Artículo 13, punto 4b) de la ley 59/2003, de 19 de diciembre, de firma electrónica

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 Procesos de solicitud de certificados

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[15]:
- 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 a los sistemas informáticos de Firmaprofesional y generar los certificados correspondientes para la propia Corporación o para sus miembros.

[15] Según el art. 18 b), de la ley 59/2003, de 19 de diciembre, de firma electrónica.

4.2 Tramitación de las solicitudes de certificados

4.2.1 Realización de las funciones de identificación y autenticación

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

4.2.2 Aprobación o denegación de las solicitudes de certificados

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.

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.

4.3 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 es necesario, la RA entregará al firmante los mecanismos necesarios para hacer uso de esos datos de generación de firma (ej, entrega física del DSCF, 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 DSCF, 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 Subscriptor 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.

4.4.2 Publicación del certificado

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

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 correspondiente.

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

No se contempla esta opción.

4.7 Renovación 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

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 reconocidos, hayan transcurrido menos de 5 años desde su última personación e identificación ante la RA[16].

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 Solicitud de renovación online

El firmante podrá contactar con la RA que emitió su certificado y solicitar su renovación. La

[16]Según el Artículo 13, punto 4b) de la ley 59/2003, de 19 de diciembre, de firma electrónica

RA le informará de cómo formalizar su solicitud.

4.7.4 Tramitación de las peticiones de renovación online

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.

4.7.5 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.

4.7.6 Forma de aceptación del certificado renovado

El certificado se aceptará al firmar electrónicamente la renovación.

4.7.7 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.

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.

4.9 Revocación y suspensión de certificados

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

La suspensión[17] 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 Causas 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.

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.
- 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.

[17] Los certificados suspendidos aparecen en la CRL con causa de revocación “Certificate Hold (6)” (RFC 3280). En algunas aplicaciones del sistema operativo Microsoft Windows, al consultar una lista de certificados revocados, dicha causa aparece traducida como “Posesión de certificado (6)”, lo cual puede inducir a error en el usuario.

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.

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.
- Por la concurrencia de cualquier otra causa especificada en la CPS.

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.

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 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 suscriptor, comunicando la hora y la causa de la misma.

4.9.3.1 Procedimiento online

Firmaprofesional pondrá a disposición del suscriptor un formulario web desde el que podrá solicitar la revocación de su certificado.

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 identifiquen.
- Introducir el Código de Revocación proporcionado durante el proceso de generación del certificado.
- Introducir la causa de solicitud de revocación.
- 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.

4.9.3.2 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.

4.9.3.3 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 y enviará un mensaje a la RA con los datos de suspensión y el motivo.

La RA dispondrá de 15 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.

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

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

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.

4.9.5 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.

4.9.6 Frecuencia de emisión de CRLs

La CRL de los certificados de entidad final se emiten al menos cada 24 horas, o cuando se produzca una revocación, con una validez de 7 días.

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

4.9.7 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.

4.9.8 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.

4.9.9 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.

4.9.10 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.

4.9.11 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.

4.9.12 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.

Adicionalmente, Firmaprofesional ofrece servicios comerciales de validación de certificados mediante el protocolo OCSP (*Online Certificate Status Protocol*) o mediante Webservices

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.

4.10.3 Características adicionales

La utilización del servicio OCSP no es público y requiere 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 ni ofrece servicios de recuperación de claves (*key scrow*).

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 de certificados ofrece protección frente:

- Accesos físicos no autorizados.
- Desastres naturales.
- Incendios.
- Fallo de los sistemas de apoyo (energía electrónica, 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 Certificación

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 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 Certificación 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 duplicado 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 los responsables

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 la norma CEN CWA 14167-1, los roles mínimos establecidos son:

- Responsable de seguridad (*Security Officer*): Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad
- Administradores del sistema de certificación (*System Administrators*): Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- Operadores de sistemas (*System Operator*): Responsables de la gestión del día a día del sistema (Monitorización, *backup*, *recovery*,…)

- Auditor interno (*System Auditor*): Autorizado a acceder a los *logs* del sistema y verificar los procedimientos que se realizan sobre el mismo.
- 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.
- Operador de RA (*Registration Officer*): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final.

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 son incompatibles en el tiempo con las tareas de Certificación e incompatibles con 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.

La CA se asegura que el personal de registro es personal confiable de una Corporación para realizar las tareas de registro. A tal efecto se exige una declaración en tal sentido por parte de la Entidad que asume funciones de RA.

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.

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 Sanciones por actuaciones no autorizadas

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

5.3.6 Requisitos de contratación de terceros

Los empleados contratados para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y la 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.

5.3.7 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 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.

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 el tiempo que se considere necesario para garantizar la seguridad del sistema en función de la importancia de cada log en concreto.

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 auditoria, 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 Análisis de vulnerabilidades

La CA realiza periódicamente una revisión de discrepancias en la información de los *logs* y actividades sospechosas, 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 auditoria,
- 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 o 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 documentos 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 solo 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

No estipulado.

5.5.7 Procedimientos para obtener y verificar información archivada

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

El acceso a la información archivada se realiza solo 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 alterara o corrompiera 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

El plan de contingencias de la jerarquía de Firmaprofesional trata el compromiso de la clave privada de la CA como un desastre.

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

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

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 21 de la Ley 59/2003 de firma electrónica, la CA podrá transferir, con el consentimiento expreso 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 certificación 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 reconocidos 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 20.1.f) de la Ley 59/2003.

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 externo.

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 Seguro de Creación de Firma (DSCF) que cumpla con los requisitos establecidos en el Art. 24 de la Ley 59/2003 de Firma Electrónica, 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 éste 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)	Periodo validez (años)
CA Raíz	4096	21
CA Subordinadas	2048	21
Entidad final	1024 / 2048	Lo establecido en la legislación y normativa vigentes
Operador / Administrador	1024 / 2048	1 (máximo)

Se está en proceso de migración de todas las claves de longitud 1024 bits a 2048 bits.

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 102 176-1.

Concretamente los parámetros utilizados son los siguientes:

Signature Suite	Hash Function	Padding Method	Signature algorithm
sha1-with-rsa	sha1	emsa-pkcs1-v1.5	rsa
sha256-with-rsa	sha256	emsa-pkcs1-v1.5	rsa

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 la claves.

Los usos admitidos de la clave para cada certificado están definidos en la Política de Certificación correspondiente.

6.2 Protección de la clave privada y controles de ingenieria 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 están certificados con la norma FIPS-140-2 nivel 3.

Las claves de los suscriptores de certificados reconocidos con DSCF y de operadores y administradores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 3, ITSEC E4 High u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor de certificados reconocidos con DSCF y del operador o administrador aportan un nivel de seguridad igual o superior al establecido por la legislación vigente para dispositivos de creación de los datos de firma. La norma europea de referencia para los dispositivos de suscriptor utilizados es CEN CWA 14169.

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.

Firmaprofesional no custodia copias de respaldo de las claves privadas de los suscriptores de certificados (*key escrow)*.

Si el suscriptor custodia las claves privadas del firmante, deberá realizarlo utilizando dispositivos criptográficos seguros certificados con la norma FIPS 140-2 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.

En otros casos, se podrá utilizar un fichero en formato PKCS12 para transferir la clave privada al módulo criptográfico. En todo caso el fichero estará protegido por un código de activación.

6.2.7 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).

6.2.8 Método de desactivación de la clave privada

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

6.2.9 Método de destrucción de la clave privada

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de las CAs, o de los datos de activación de las mismas.

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 periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación este 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 de mantener la confidencialidad de estos datos.

6.5 Controles de seguridad informática

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

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 auditoria.
- Auditoria 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 la gestión de este material para garantizar su uso.

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 perdida de efectividad de un certificado digital de forma permanente. La revocación se realizara 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.

6.6.2.9 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 catalogo 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 test de 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

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 trasfiere por redes no seguras se realiza de forma cifrada.

6.8 Fuente de tiempo

El tiempo se obtiene mediante consulta al Real Observatorio de la Armada[18], siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en el RFC 1305 "*Network Time Protocol*".

[18] Información del sitio web:
http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/06_Hora

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 TS 101 862 conocida como “European profile for Qualified Certificates”
- RFC 3280 "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	Nº de versión	V3 (versión del estándar X509)
Serial	nº de serie	Código aleatorio único con respecto al DN del emisor
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	Digital Signature Non Repudiation Key Encipherment, Data Encipherment, Key Agreement
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	id de la clave pública del certificado, obtenido a partir del hash de la misma

Extensión	Crítica	Posibles Valores
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 correspondiente al certificado. URI de la CPS User Notice : Nota de texto que se puede desplegar en la pantalla del usuario
QcStatements	-	Existen 3 tipos: Id-etsi-qcs-QcCompliance (a añadir cuando el certificado es reconocido) Id-etsi-qcs-QcSSCD (indica que la clave privada se guarda en un DSCF) id-etsi-qcs-QcLimitValue: Límite del valor de las transacciones
X509v3 Subject Alternative Name	-	(opcional) email del firmante
X509v3 Issuer Alternative Name	-	(opcional) URI:http://www.firmaprofesional.com
X509v3 Authority Information Access	-	(opcional) URI dónde se encuentra el certificado de la CA (opcional) URI del servicio OCSP
1.3.6.1.4.1.13177.10.1.5.1.1	-	(Obsoleto) Extensión propietaria de Firmaprofesional . Puede tener el valor 'Mancomunado' si la firma de la persona jurídica es mancomunada. En caso de no ser necesaria firma mancomunada no aparecerá la extensión
1.3.6.1.4.1.13177.10.1.5.1.2	-	(Obsoleto) Extensión propietaria de Firmaprofesional que incluye los datos de inscripción registral del suscriptor
netscape-cert-type	-	(Obsoleto)
netscape-comment	-	(Obsoleto)

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 la política de certificación de cada tipo de certificado se especificará las extensiones requeridas.

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
1.2.840.113549.1.1.11	sha256withRSAencryption	OID del algoritmo de firma

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 ".

E, E-mail	E-mail	Correo electrónico del firmante
ST, State	Ubicación Geográfica	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*
SN, surName	Apellidos	Apellidos del Firmante
GN, givenName	Nombre de Pila	Nombre del Firmante

(*) En caso de que el firmante no disponga de NIF o NIE, contendrá un código de documento con el siguiente formato <P>-<T>-<XXXXXX>, donde:

- <P> Código del país (según ISO 3166-1)
- <T> es el tipo de documento (P para pasaporte)
- <XXXXXXXX> es el código del documento (el identificador utilizado en el país en el que está dada de alta la entidad a la que está vinculado el sujeto)

7.1.5 Restricciones de los nombres

Respecto a la codificación de los certificados, y siguiendo el estándar RFC 3280 ("*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.*X.Y*, donde los 2 últimos dígitos (X e Y) indican la versión (mayor y menor respectivamente) del documento.

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

7.1.7 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.

7.1.8 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 3280 "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 (CA Root)

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha1WithRSAEncryption
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	Sha1WithRSAEncryption
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 dias
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 la política de certificación de Servicio Seguro (TSA/VA).

8 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia de las auditorias

Se realizarán auditorias periódicas, generalmente con carácter anual.

8.2 Cualificación del auditor

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

Desde el año 2003, Firmaprofesional dispone de la certificación *WEBTRUST for Certification Authorities*, que se pueden descargar y consultar en http://www.aicpa.org, desarrollados por la AICPA (American Institute of Certified Public Accountants, Inc.) y la CICA (Canadian Institute of Chartered Accountants).

La auditoría necesaria para obtener la certificación *WebTrust* fue realizada por la prestigiosa compañía *Ernst&Young S.L.* (*Technology and Security Risk Services*)

Firmaprofesional se compromete a realizar las auditorias necesarias para mantener vigente dicha certificación.

Los principios y criterios *WebTrust* para CA son consistentes con los estándares desarrollados por la *American National Standards Institute* (ANSI) y la *Internet Engineering Task Force* (IETF).

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.

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 auditorias 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:

a. 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.

b. 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 por un tercero previamente a su puesta en marcha efectiva. Adicionalmente, se realizan auditorias 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 incidencias

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 formador 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 alguna tarifa para los casos de 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.

Firmaprofesional ofrece otros servicios de validación de certificados comerciales (como OCSP o Webservices), 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.

9.2 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.

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura de 3.000.000 €.

Dichas garantías no son aplicables a los certificados que no sean reconocidos, 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 €.

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 la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

Según lo dispuesto en el artículo 19.3 de la ley 59 /2003 de Firma electrónica, esta CPS deberá considerarse el "Documento de Seguridad" a los efectos previstos en la legislación sobre protección de datos y su desarrollo normativo.

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 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 Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal, Firmaprofesional dispone del fichero BB DD CERTIFICADOS, cuya finalidad es la gestión de los certificados emitidos y la prestación de los servicios de certificación asociados.

Información del fichero:

Nombre	BB DD CERTIFICADOS
Nº de inscripción en el Registro General de Protección de Datos	2022130054
Servicio de atención al público	Edificio ESADECREAPOLIS Avenida Torre Blanca, 57. Sant Cugat del Valles 08173

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 Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Concretamente, las siguientes secciones recogidas en ***TÍTULO VIII "De las medidas de seguridad en el tratamiento de datos de carácter personal" del Real Decreto 1720/2007*** cumplen en las secciones especificadas del presente documento y en el documento de Política de Seguridad:

a) Ámbito de aplicación del documento de seguridad → sección 9.4

b) Nivel de seguridad aplicable → secciones 5, 6 y 9.4

c) Funciones y obligaciones del personal → sección 5.3

d) Estructura de los ficheros de datos de carácter personal → sección 9.4

e) Notificación y gestión de incidencias → Política de Seguridad

f) Copias de seguridad y recuperación → Política de Seguridad

Se cumple así con lo dispuesto en el artículo 19.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que considera la declaración de prácticas de certificación como documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal.

9.4.2 Información tratada como privada

De conformidad con lo establecido en el artículo 3 de la ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se consideran datos de carácter personal 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 básico.

9.4.2.1 Estructura de los 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, titulo 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 la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

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 a datos propiedad Firmaprofesional que asume las medidas de índole técnica, organizativa y de seguridad que garanticen la confidencialidad e integridad de la información de acuerdo con lo establecido en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, y demás legislación aplicable.

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 prejuicio de las demás acciones legales.

Cualquier usuario registrado puede en cualquier momento ejercer el derecho a acceder, rectificar y, en su caso, cancelar sus datos de carácter personal suministrados a

Firmaprofesional mediante comunicación escrita con referencia "tratamiento 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 si se incurre en los casos recogidos en el punto 2 del artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

9.4.7 Otras circunstancias de publicación de información

Aquéllas descritas en el punto 2 del artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

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.

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

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 y la Ley 59/2003, principalmente a:

a) Respetar lo dispuesto en las Políticas y Prácticas de Certificación (la presente CPS), así como en las Condiciones Generales de emisión.

b) Publicar esta CPS 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 reconocidos 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, 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).

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.

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 y de la CP correspondiente al certificado.

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

e) Formalizar el contrato de certificación con el subscriptor 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, 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.

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.

9.6.4 Obligaciones de los firmantes

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

a) Custodiar sus DSCF, claves privas 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.

9.6.5 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.

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.

9.7 Exención de garantía

Firmaprofesional puede rechazar toda garantía de servicio que no se encuentre vinculado a las obligaciones establecidas por la ley 59/2003, de 19 de diciembre.

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 59/2003, de 19 de diciembre, de firma electrónica o su normativa de desarrollo.

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 y en la Ley 59/2003, de 19 de diciembre, de firma electrónica y su normativa de desarrollo, donde sea aplicable.

Firmaprofesional será responsable del daño causado ante el Suscriptor 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 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 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.

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

Cualquier elemento de esta CPS puede ser cambiado unilateralmente por Firmaprofesional sin preaviso. Las modificaciones deben estar justificadas desde un punto de vista legal, técnico o comercial.

9.12.1.3 Mecanismo de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los suscriptores, usuarios u 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

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

9.15 Cumplimiento de la normativa aplicable

Firmaprofesional manifiesta el cumplimiento de la ley 59/2003, de 19 de diciembre, de firma electrónica.

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 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.