Signe - Autoridad de Certificación

Política de certificación

Certification policy

Declaración de Prácticas de Certificación

Versión 2.0

Fecha: 28/02/2018

Seguridad documental

Versión	Cambios	Fecha
1.0	Creación del documento	02/11/2010
1.1	Cambios en el formato	24/03/2015
1.2	Cambios del documento	06/06/2016
1.3		01/07/2016
1.4	Cambios en longitud de claves y algoritmo hash	14/10/2016
2.0	Adaptación a eIDAS	28/02/2018

Índice

1. Introducción

1.1. Presentación

Signe S.A. (en adelante SIGNE) es una mercantil cuya actividad principal es la prestación de servicios consistentes en la edición e impresión de documentos de seguridad para empresas públicas y privadas. Desde el año 2010, SIGNE inicia su actividad como Prestador de Servicios de Certificación (PSC) que emite certificados reconocidos según la Ley 59/2003, de 19 de diciembre, de firma electrónica.

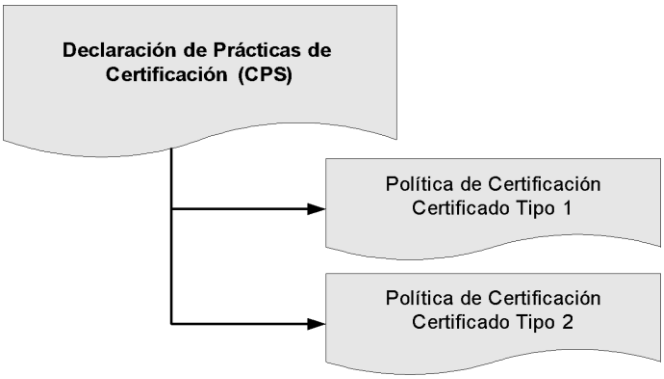
Los servicios de Certificación Electrónica ofrecidos por SIGNE están orientados a los egresados, estudiantes que han completado sus estudios y se encuentran en situación de obtener el título que acredite la consecución de los mismos, y a Corporaciones Públicas y Privadas (como empresas, entidades públicas, universidades u otros centros académicos docentes).

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 (DPC) de SIGNE, (en inglés CPS o Certification Practice Statement).

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

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

Existe una política de certificación y un texto de divulgación por cada tipo de certificado emitido.



SIGNE adecua sus servicios de certificación al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

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

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

- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)

1.2. 2 Nombre del documento e identificación

1.2.1. Identificación

Nombre:	Declaración de Practicas de Certificación (DPC)
Versión:	2.0
Descripción:	Declaración de Prácticas de Certificación de Signe S.A.
Fecha de Emisión:	28/02/2018
OID	1.3.6.1.4.1.36035.0.1.0
Localización	https://www.signe.es/signe-ac/dpc

1.2.2. OIDs

Siguiendo los estándares de certificación digital, SIGNE 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".*

SIGNE tiene registrado en IANA el número "**36035**" como OID de empresa privada (http://www.iana.org/assignments/enterprise-numbers). El significado de los OID que comienzan por "1.3.6.1.4.1.36035" es el siguiente:

OID	Tipo de Objeto	Descripción
0.V.R	Declaración de Prácticas de Certificación (DPC)	V = Versión de la DPC R = Subversión de la DPC
1.T.D	Políticas de Certificación de emisión de certificados	T = Tipo de Certificado: 1 = de Titulado 2 = Corporativo de Persona Física 5 = Corporativo de Sello Empresarial 10 = Sello de Órgano D = Dispositivo: 1 = DCCF portable 2 = Software 3= DCCF centralizado
2	Política de Certificación de CA Subordinada	CA Subordinada
3.1.T.N	Campo con información relativa a la titulación	T = identifica a la información correspondiente a una misma titulación: N=1: nombre oficial de la titulación N=2: código oficial de la titulación N=3: organismo que ha expedido la titulación

1.3. Entidades participantes

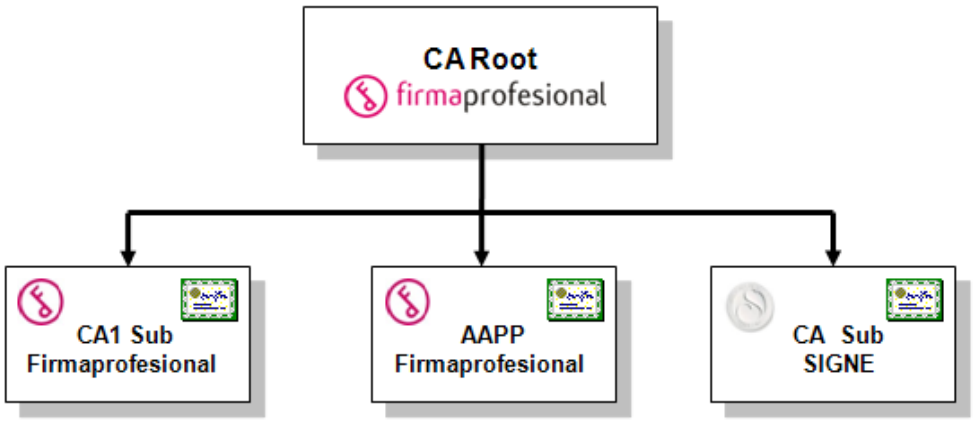
1.3.1. Prestador de Servicios de Certificación (PSC)

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

SIGNE 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 SIGNE.

1.3.2. Autoridad de Certificación (CA)

SIGNE forma parte de la Jerarquía de Certificación de Firmaprofesional, que está compuesto por diversas Autoridades de Certificación (en inglés CA o *Certificate Authority*).



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 Certificación 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

Autoridades de Certificación Subordinadas

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.

En tanto que es Prestador de Servicios de Certificación, SIGNE dispone de una Autoridad de Certificación Subordinada. 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* y *Mozilla CA Certificate Inclusion Policy* vigentes en el momento de entrada en vigor de la presente CPS.

CN = SIGNE Autoridad de Certificación

Hash SHA1: *D730 47F2 CCE5 64EF B0BC 8568 93EA 19D7 7469 398C*

Válido desde el 21 de Julio 2010 al 21 de Julio de 2022

Longitud de clave RSA 2048 bits

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*

La Autoridad de Certificación Subordinada "**SIGNE Autoridad de Certificación**" emite certificados digitales a personas físicas, a corporaciones privadas y a corporaciones públicas, conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Públicos.

1.3.3. Autoridad de Registro (RA)

Una Autoridad de Registro (en inglés RA o *Registration Authority*) dentro del Sistema de Certificación de SIGNE, 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 SIGNE:

- La propia SIGNE directamente.
- Cualquier Corporación que sea cliente de SIGNE, 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 SIGNE para actuar como intermediario en nombre de SIGNE.

SIGNE formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como RA dentro del Sistema de Certificación de SIGNE.

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

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 SIGNE.

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 SIGNE. Por lo tanto será el propietario del certificado.

Concretamente:

- En el caso de certificados **Personales**, el Suscriptor es la persona física titular del certificado.
- En el caso de certificados **Corporativos**, el Suscriptor es siempre una Corporación (empresa privada, entidad pública, universidad), que ha contratado los servicios de certificación de SIGNE. En este caso la Corporación es la propietaria del certificado.

1.3.6. Firmante

El Firmante se trata de la persona física que posee un dispositivo de creación de firma o control sobre el mismo, en caso de ser remoto, y que actúa en su nombre y derecho, o bien como sujeto que pertenece a una Administración Pública, organismo o entidad de derecho público, suscriptor del certificado.
El Firmante será responsable de custodiar los datos de creación de firma, es decir, la clave privada asociada al certificado.

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, *relaying party*) a toda persona u organización que voluntariamente confía en el certificado de entidad final emitido por SIGNE.

La Autoridad de Certificación SIGNE está subordinada a la Autoridad de Certificación Raíz de Firmaprofesional, entidad con la que comparte la mayoría de prácticas de certificación debido al acuerdo de prestación de servicios entre ambas. Por ello, las entidades que confíen en la Autoridad de Certificación Raíz de Firmaprofesional pueden confiar en los certificados emitidos por SIGNE.

El certificado Raíz de Firmaprofesional está reconocido por **Microsoft** en todas sus aplicaciones, incluyendo Internet Explorer, y por la Fundación Mozilla, incluyendo el navegador **Firefox.**

Adicionalmente, SIGNE tratará de establecer acuerdos con el mayor número de entidades posible, como Ministerios, CCAA, Diputaciones o Ayuntamientos, para el reconocimiento de los certificados reconocidos en sus aplicaciones.

Las obligaciones y responsabilidades de SIGNE con terceros que voluntariamente confíen en los certificados se limitarán a las recogidas en esta DPC, en la Ley 59/2003 de Firma Electrónica, y en el Reglamento UE 910/2014, y deberán tener presente las limitaciones en su uso.

1.4. Tipos de certificados

1.4.1. Certificados Personales reconocidos / cualificados

Certificado de Titulado: son certificados personales reconocidos según la Ley 59/2003 de firma electrónica y cualificados según el RD UE 910 / 2014 que permiten identificar telemáticamente al SUSCRIPTOR como poseedor de una determinada titulación académica.

Estos certificados son emitidos en soporte software, a través de una aplicación, obteniendo un certificado para la firma y la autenticación. Pueden además ser copiados a otros soportes, siendo por lo tanto posible realizar copias de seguridad de los mismos.

OID DE POLITICAS DE CERTIFICADOS PERSONALES	
1.3.6.1.4.1.36035.1.1.D	CP de Titulado

D = Dispositivo/Nivel de Seguridad:
1 = DCCF portable, 3 = DCCF centralizado, 2 = Otros dispositivos

1.4.2. Certificados Corporativos cualificados

Los Certificados Corporativos son certificados reconocidos según la Ley 59/2003 de firma electrónica, y cualificados según el RD UE 910/2014 cuyo Suscriptor es una Corporación (ya sea una empresa, una organización, un colegio profesional o una Administración Pública):

- **Certificados Corporativos de Persona Física**: Son certificados cualificados de persona física que identifican al Suscriptor como Corporación y al firmante como vinculado a esa Corporación, ya sea como empleado, asociado, colaborador, cliente o proveedor.
- **Certificados Corporativos de Sello Empresarial**: Son certificados electrónicos emitidos a personas jurídicas de conformidad con el artículo 38 del Reglamento UE 910/2014.

OID DE POLÍTICAS DE CERTIFICADOS CORPORATIVOS	
1.3.6.1.4.1.36035.1.2.D	CP Corporativo de Persona Física

1.3.6.1.4.1.36035.1.5.D	CP Corporativo de Sello Empresarial

D = Dispositivo/Nivel de Seguridad:
1 = DCCF portable, 3 = DCCF centralizado, 2 = Otros dispositivos

1.4.3. Certificados para la Administración Pública

Los Certificados para la Administración Pública son certificados electrónicos emitidos de acuerdo con la Ley 40/2015.

- **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. Son certificados acorde con el Anexo III del Reglamento UE 910/2014 y el artículo 40 de la Ley 40/2015

OID DE POLITICAS DE CERTIFICADOS PARA LA ADMINISTRACION PÚBLICA	
1.3.6.1.4.1.36035.1.10.D	CP Sello de Órgano

D = Dispositivo/Nivel de Seguridad:
1 = DCCF portable - Nivel Alto, 3 = DCCF centralizado - Nivel Alto, 2 = Otros dispositivos - Nivel Medio

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 Prácticas de Certificación y en su correspondiente Política de Certificación.

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

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

SIGNE no ofrece el servicio de recuperación de la clave privada, 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, SIGNE tenga responsabilidad alguna por pérdida de información derivada de la pérdida de las claves de cifrado. Por ello, SIGNE no recomienda el uso de los certificados digitales para el cifrado de la información.

1.6 1.6. Administración de las políticas

1.6.1. Organización responsable

El Departamento Técnico de SIGNE constituye la autoridad de las políticas (AP) de SIGNE y es responsable de la administración de esta DPC y de las Políticas de Certificación.

1.6.2. Persona de contacto

Organización responsable:	Signe, S.A.
Persona de contacto:	Director Técnico de SIGNE
E-mail:	signe-ac@signe.com
Teléfono:	+34 902 30 17 01
Dirección:	SIGNE S.A. Avda. de la Industria, 18 Tres Cantos 28760 Madrid

1.6.3. Frecuencia de revisión

La DPC y las distintas PC y PDS serán revisadas y si procede, actualizadas, anualmente.

1.6.4. Procedimiento de aprobación

La publicación de las revisiones de esta DPC y de las Políticas de Certificación y Textos de Divulgación-PDS de cada tipo de certificado deberá ser aprobada por la *Autoridad de las políticas* de SIGNE, 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.

Certificado Cualificado: Certificado expedido por un Prestador Cualificado de Servicios de Confianza y que cumple los requisitos establecidos en el Anexo I del RD UE 910/2014.

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 Suscriptor utiliza para crear la Firma

electrónica.

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

Dispositivo Cualificado de Creación de Firma / de Sello electrónico (DCCF): Dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

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

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

Firma Electrónica Reconocida/Cualificada: es aquella firma electrónica avanzada basada en un certificado reconocido/cualificado y generada mediante un dispositivo seguro/cualificado de creación de firma.

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

Listas de Certificados Revocados: lista donde figuran las relaciones de certificados revocados o suspendidos.

Módulo Criptográfico Hardware: módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

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

Sello Cualificado de Tiempo Electrónico: es un sello de tiempo electrónico que cumple los requisitos establecidos en artículo 42 del RD UE 910/2014.

Autoridad de sellado de Tiempo: Entidad de confianza que emite sellos de tiempo.

Autoridad de Validación: 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
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
DPC:	Declaración de Prácticas de Certificación (Certificate Practice Statement)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
OID:	Identificador de objeto único (Object identifier)
PDS	Texto de Divulgación (PKI Disclousure Statement)
PC:	Política de Certificación (Certificate Policy)
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)

Estándares y Organismos de estandarización

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

PKIX: Grupo de trabajo del IETF sobre PKI

PKCS: Public Key Cryptography Standards

RFC: Request For Comments

2. Repositorios y publicación de información

2.1. Repositorios

Acceso	Descripción	URL
Público	DPC y Políticas de Certificación y PDS	https://www.signe.es/signe-ac/dpc
Público	CA Raíz Firmaprofesional (con caducidad 2030)	https://www.signe.es/signe-ac/crl/caroot.crt
Público	CA Subordinada SIGNE	https://www.signe.es/signe-ac/crl/signe.crt
Público	ARL: Lista de CAs Revocadas (emitida por la CA Raíz 2030)	https://www.signe.es/signe-ac/crl/fproot.crl
Público	CRL: Lista de Certificados Revocados de usuario final	https://www.signe.es/signe-ac/crl/signe.crl
Público	Servicio de Revocación	https://www.signe.es/signe-ac/obtencion-renovacion-revocacion/
Público	Servicio de Validación (OCSP)	https://servicios.signe.es/ocsp

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

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

2.2. Publicación de información

2.2.1. Políticas y Prácticas de Certificación

Tanto la DPC actual como las Políticas de Certificación y los Textos de Divulgación de cada tipo de certificado estarán disponibles en formato electrónico en la Web de SIGNE.

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

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

2.2.2. Términos y condiciones

La relación contractual entre SIGNE y los Suscriptores está basada en la firma de un **Contrato de Prestación de Servicios de Certificación** y la aceptación de la Declaración de Prácticas de Certificación y las CP y PDS que correspondan de SIGNE publicadas en su web https://www.signe.es/signe-ac/dpc.

2.2.3. Difusión de los certificados

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

2.3. Frecuencia de publicación

Según la Declaración de Prácticas de Certificación de Firmaprofesional, 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.

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

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

2.4. Control de acceso a los repositorios

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

Los certificados emitidos se publican en repositorios públicos. Dicha publicación debe realizarse siempre que el suscriptor o firmante del certificado consienta de forma expresa esta acción.

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

3. Identificación y Autenticación

3.1. Registro de Nombres

3.1.1. Tipos de nombres

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

- ETSI TS 101 862 conocida como “European profile for Qualified Certificates”
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- RFC 3739 “QualifiedCertificatesProfile”.

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 Suscriptor, 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

SIGNE no emite certificados de seudónimo.

3.1.4. Reglas para interpretar varios formatos de nombres

SIGNE 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 usa 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. SIGNE 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 Suscriptor.

Cada RA es responsable de garantizar la entrega del dispositivo al Suscriptor 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 SIGNE.

3.2.2. Autenticación de la identidad de una persona jurídica

La Autoridad de Registro verificará 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.

La RA podrá verificar los datos anteriores según uno de los siguientes procedimientos:

- Mediante conexión telemática con los correspondientes registros públicos o especiales (por ejemplo con un acceso en línea al Registro Mercantil).
- Mediante la solicitud de las escrituras públicas, contratos, estatutos, pactos o cualesquiera otros documentos que puedan acreditar su constitución, vigencia e identificación de los miembros que las integran.

SIGNE 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 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:

- SIGNE verificará la existencia de la entidad mediante sus propias fuentes de información.
- Un representante autorizado de la organización deberá firmar un contrato con SIGNE, 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 SIGNE 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 con la RA se realiza de forma segura mediante el uso de certificados digitales de operador.

3.2.5. Validación del correo electrónico

Para los certificados Personales, se valida la dirección de correo electrónico mediante desafío y respuesta a la dirección proporcionada por el Solicitante.

3.3. Identificación y autenticación en la renovación de certificados

3.3.1. Renovación de certificados online

El Suscriptor 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[1].

Los requisitos específicos podrán diferir según el tipo de certificado solicitado y estarán recogidas en la "**Política de Certificación**" del tipo de certificado 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 Suscriptores en el proceso de revocación de certificados podrá ser realizada por:

a) **El propio Suscriptor**: identificándose y autenticándose mediante el uso del

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

Código de Revocación en la página web de SIGNE.

b) RA de SIGNE: deberá identificar al Suscriptor ante una petición de revocación según los propios medios que considere necesarios.

4. Requisitos operacionales en el ciclo de vida de los certificados

4.1. Solicitud de certificados

4.1.1. Quién puede solicitar un certificado

El certificado podrá ser solicitado por el Solicitante. Los requisitos que debe reunir un Solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "**Política de Certificación**" de cada tipo de certificado concreto.

4.1.2. Proceso de solicitud de certificados

El Solicitante deberá ponerse en contacto con una RA deSIGNE para gestionar la solicitud del certificado.

La RA proporcionará al Solicitante la siguiente información[2]:

- Documentación necesaria a presentar para la tramitación de su solicitud y para verificar la identidad del Suscriptor.
- 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, las Políticas de Certificación y las Condiciones Generales de Contratación.

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

[2] 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 Suscriptor. 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 Suscriptor.

Si la información no fuese correcta, la RA deberá denegar la petición, contactando con el solicitante para comunicarle el motivo.

Si es correcta, y en el caso de la emisión de un Certificado Personal, se procederá a la firma del instrumento jurídico vinculante entre el Suscriptor y SIGNE. En el caso de la emisión de Certificados Corporativos, SIGNE verificará que el instrumento jurídico existe y que ha sido firmado, siendo responsabilidad del Solicitante verificar que el Firmante pertenece a la Corporación.

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

Una vez aprobada la solicitud se procederá a la emisión del certificado, que deberá ser entregado de forma segura al Suscriptor.

a) Para los certificados en soporte *hardware*:
   - La RA le hará entrega o verificará que el solicitante posee un DCCF que cumpla los requisitos establecidos en la ley[3] y un dispositivo de acceso a él, si los hubiera (generalmente un lector de tarjetas). En caso de que el solicitante aporte su propio dispositivo, éste deberá ser homologado por SIGNE previamente a su utilización. SIGNE dispondrá de una lista pública de dispositivos homologados.
   - Activación del dispositivo: En el caso que el Solicitante no disponga de ellos, se generarán los datos de activación del dispositivo y de acceso a la clave privada que contendrá el mismo.
   - Generación del par de claves: Se procederá a la generación de las claves utilizando el sistema proporcionado por la RA.

b) Para los certificados en *software*:
   - La RA indicará al Solicitante los pasos a seguir para generar el par de claves en el navegador.
   - Se proporcionará un código de autenticación al Solicitante que deberá presentar para proceder con la emisión del certificado.

c) En ambos casos:
   - La RA verificará el contenido de la petición de certificado, y si la verificación es correcta validará la petición.
   - Se enviará por un canal seguro la clave pública junto con los datos verificados a la CA en formato PKCS10 u otro equivalente. Se procederá entonces a la generación del certificado en un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.
   - Entrega del certificado: El certificado generado será enviado a la RA, que lo pondrá a disposición del Suscriptor.
   - Durante la generación de los certificados, la CA se encargará de añadir las informaciones restantes establecidas necesarias para cumplir con los requisitos legales establecidos.

[3] Art. 24 de la ley 59/2003, de 19 de diciembre, de firma electrónica.

4.3.2. Notificación al Suscriptor por la CA de la emisión del certificado

La CA notificará al Suscriptor 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 SIGNE haya sido firmado y el certificado haya sido entregado, ya sea personal o telemáticamente.

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

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

4.4.2. Publicación del certificado

Una vez el certificado esté generado y aceptado por el Suscriptor, el certificado podrá ser publicado en los repositorios de certificados que se consideren necesarios, siempre que el suscriptor o firmante no se haya opuesto a dicha publicación.

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 DPC y en la Política de Certificación y Texto de Divulgación (PDS) correspondientes.

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

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

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

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por SIGNE 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:

- El certificado no ha caducado.
- Hayan transcurrido menos de 5 años desde su última personación e identificación ante la RA[4]. En ciertos casos esta condición podrá obviarse si se

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

utiliza para ello el DNIe. Los detalles de la renovación pueden encontrarse en las Políticas de Certificación correspondientes.

4.7.2. ¿Quién puede pedir la renovación online de un certificado?

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

4.7.3. Solicitud de renovación online

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

4.7.4. Tramitación de las peticiones de renovación online

Se realizarán los siguientes pasos:

- Se notificará al Suscriptor por correo electrónico de que puede renovar su certificado.
- Se solicitará a los Firmantes que se conecten a una página web de renovaciones. Mediante el uso de su certificado deberán firmar 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 Firmante y el anterior será revocado.

4.7.5. Notificación de la emisión del certificado renovado

La CA notificará al Suscriptor que el certificado ha sido renovado al finalizar correctamente el proceso.

El certificado se aceptará al firmar electrónicamente la renovación.

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, siempre que el firmante no se hubiera opuesto

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

No se contempla la suspensión de certificados. SIGNE no realiza suspensiones de certificados.

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 o cambio del Firmante de la vinculación con la Corporación, en

el caso de Certificados Corporativos.

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 DPC.
   - 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 incumplimiento por parte del Suscriptor de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre la CA, la RA y el Suscriptor.

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.
   - El incumplimiento por parte del Suscriptor de las normas de uso del dispositivo criptográfico expuestas en la presente DPC, en las condiciones generales de contratación o en el instrumento jurídico vinculante entre la CA, la RA y el Suscriptor.

d) Circunstancias que afectan al **Suscriptor**:
   - Finalización de la relación jurídica entre la CA, la RA y el Suscriptor.
   - Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al Suscriptor.
   - Oposición o modificación, por parte del Firmante, de los datos contenidos en el fichero de datos de carácter personal de SIGNE.
   - 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 las condiciones generales de contratación.
   - La incapacidad sobrevenida, total o parcial por el fallecimiento del

Suscriptor.

e) Otras circunstancias:
   - Por resolución judicial o administrativa que lo ordene.
   - Por la concurrencia de cualquier otra causa especificada en la DPC.

4.9.2. Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

a) El propio Suscriptor, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.
b) 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 autorizados de la RA a la que pertenece el Suscriptor del certificado.
- Los operadores autorizados de la CA.

4.9.3. Procedimientos de solicitud de revocación

Existen distintas alternativas para el Suscriptor o el firmante a la hora de solicitar la revocación del certificado.
En todo caso, al tiempo de revocarse el certificado, se enviará un comunicado al Suscriptor y al firmante, comunicando la hora y la causa de la misma.

4.9.3.1. Procedimiento online

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

Mediante el formulario, SIGNE solicitará al Suscriptor:
- Datos que le identifiquen.
- El código de revocación del certificado 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 telefónica

SIGNE pone a disposición del Suscriptor un servicio de revocación telefónico en el que podrá solicitar la revocación de su certificado:

Servicio de revocación Horario de Oficina: 902 30 17 01

La RA identificará y autenticará al Suscriptor mediante una serie de preguntas personales. Una vez correctamente identificado, el operador procederá a efectuar la revocación.

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

Una vez la identidad del Suscriptor 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”.
- Se deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.
- Se deberá comprobar que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.

- Los certificados revocados que expiren son retirados de la CRL.

También se puede comprobar las revocaciones por medio del servicio OCSP.

4.10. Servicios de información del estado de certificados

4.10.1. Características operativas

Con el fin de proporcionar información sobre la validez de un certificado electrónico, y por consiguiente de la fiabilidad de la firma electrónica de un documento, SIGNE ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

SIGNE ofrece un servicio gratuito de acceso a validación de certificados en línea por medio del protocolo OCSP.

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

4.10.2. Disponibilidad del servicio

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

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

4.10.3. Características adicionales

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

4.11. Finalización de la suscripción

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

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

SIGNE subcontrata a Firmaprofesional el hosting, la gestión y operación de sus servicios de certificación. Con ello, SIGNE se adhiere a la Declaración de Prácticas de Certificación de Firmaprofesional, concretamente a su apartado 5º: CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES, del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN de Firmaprofesional, S.A., en su versión 5.0 publicada el 26 de Julio de 2010, que se transcribe íntegramente a continuación.

5.1. Controles físicos

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

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

- Accesos físico 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 las normas ETSI EN 319 401 y 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.
- Operador de RA (*Registration Officer*): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final, así como las oportunas verificaciones en certificados de autenticación web.
- Responsable de revocación (*Revocation Officers*): Responsable de realizar los cambios en el estado de un certificado.
- 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 (*SystemOperator*): 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.

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.

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

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.

Tanto Firmaprofesional como SIGNE retirarán 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 y SIGNE realizan 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 a acceder a los sistemas de la RA.

5.3.3. Requerimientos de formación

Firmaprofesional y SIGNE realiza los cursos necesarios a sus empleados y a los operadores de la RA 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 DPC, que serán notificadas a medida que sean aprobadas.

5.3.5. Frecuencia y secuencia de rotación de tareas

Sin estipulación adicional.

5.3.6. Sanciones por actuaciones no autorizadas

Tanto Firmaprofesional como SIGNE disponen de un régimen sancionador interno por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

5.3.7. Requisitos de contratación de terceros

Los empleados contratados para realizar tareas confiables deberán firmar con anterioridad las cláusulas de confidencialidad y 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.

5.3.8. Documentación proporcionada al personal

Firmaprofesional y SIGNE 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

SIGNE 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, SIGNE registra:

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

SIGNE conserva, ya sea física 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 durante 15 años para garantizar las 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 auditoría, realizando semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena en armario ignífugo bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado. Se realizan copias diarias incrementales y completas semanales.

Adicionalmente se mantiene copia de los logs de auditoría en un 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 auditoría.
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores y los datos relativos a su identificación.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos o publicados.
- CRL's emitidas o registros del estado de los certificados generados.
- La documentación requerida por los auditores.
- 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. En particular:

- 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 (desde el momento de la caducidad del certificado) 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 DPC, 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, SIGNE procederá según lo estipulado en el documento "Política de seguridad[5]".

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 SIGNE trata el compromiso de la clave privada de la CA como un desastre.

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

- 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.

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

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 DPC 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] Documento disponible en www.signe.es/signe-ac/dpc/

5.8. Cese de actividad

5.8.1. Autoridad de Certificación

Antes del cese de su actividad SIGNE 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.

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

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

5.8.2. Autoridad de Registro

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

- 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 SIGNE.

6. Controles de seguridad técnica

SIGNE subcontrata a Firmaprofesional el hosting, la gestión y operación de sus servicios de certificación. Con ello, SIGNE se adhiere a la Declaración de Prácticas de Certificación de Firmaprofesional, concretamente a su apartado 6º: CONTROLES DE SEGURIDAD TÉCNICA, del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN de Firmaprofesional, S.A., en su versión 5.0 publicada el 26 de Julio de 2010, que se transcribe íntegramente a continuación.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Se distinguirán dos casos en la generación de claves para certificados reconocidos:

a) En hardware (soporte físico)

- 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, el par de claves será creado en el mismo dispositivo utilizando el sistema proporcionado por la RA. Este proceso está vinculado de forma segura al proceso de generación del certificado, garantizando la confidencialidad de la clave privada durante el proceso de generación y la complementariedad entre los datos de creación y verificación de firma[6].

[6] Conforme con el art. 20, punto 1e), y con el art. 12 puntos c) y d), de la ley 59/2003, de 19 de diciembre, de firma electrónica.

b) En software

- El Suscriptor recibirá una invitación para conectarse al servicio de generación de certificados. El Suscriptor generará el par de claves en su sistema y enviará la clave pública a la CA en formato PKCS10 u otro equivalente.

En otros casos, la generación de claves del Suscriptor se realizará en dispositivos que aseguran razonablemente que la clave privada será protegida por el Suscriptor contra la utilización por otros, bien por medios físicos, bien estableciendo el Suscriptor los controles y medidas de seguridad adecuadas.

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

6.1.2. Entrega de la clave privada al Suscriptor

a) En hardware (soporte físico)

- La clave privada será entregada junto al certificado en el dispositivo de creación de firma.
- La RA será responsable de garantizar la entrega del dispositivo al Suscriptor, 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[7].
- El dispositivo criptográfico utiliza una clave de activación para el acceso a las claves privadas. En caso de que la entrega del dispositivo no se realice de manera presencial ante la RA, los datos de activación se enviarán al lugar de entrega del dispositivo por separado.

b) En software

- Las claves serán generadas por el Solicitante, o por la RA en los sistemas indicados por el Solicitante, utilizando aplicaciones compatibles con los estándares de PKI, haciendo entrega a la RA de una petición de certificado en formato PKCS#10.

[7] Conforme con el art. 20, punto 1e), y con el art. 12 punto c) de la ley 59/2003, de 19 de diciembre, de firma electrónica.

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 SIGNE.

6.1.5. Tamaño de las claves

Certificado	Tamaño claves RSA (bits)	Periodo validez (años)
CA Raíz	4096	21
CA Subordinadas	2048	12
Entidad final	1024 / 2048 (*)	4 (máximo)
Operador/Administrador	1024 / 2048 (*)	1 (máximo)

(*) Únicamente 2048 desde 1 de enero de 2017

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 la ETSI TS 119 312.

Concretamente los parámetros utilizados son los siguientes:

entry name of the signature suite	entry name for the hash function	entry name for the padding method	entry name for the signature algorithm
sha256-with-rsa	sha256	No padding required	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 ingeniería de los módulos criptográficos

6.2.1. Estándares para los módulos criptográficos

Los módulos criptográficos empleados para generar y almacenar las claves de las Autoridades de Certificación están certificados con la norma FIPS-140-2 nivel 3.

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

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

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.

SIGNE 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 según las indicaciones expuestas en el punto 6.2.1 y garantizando en todo momento el uso exclusivo de las claves por parte del firmante.

6.2.4. Copia de seguridad de la clave privada

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

Este procedimiento se describe en detalle en las políticas de seguridad de SIGNE [8].

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

[8] Disponible en www.signe.es/signe-ac/dpc/

Documento disponible en www.firmaprofesional.com/cps

archivadas por un periodo de al menos 10 años, después de la emisión del último certificado.

Las claves privadas de los Suscriptores pueden ser archivadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación. La CA no archivará nunca las claves privadas de los certificados reconocidos de los Suscriptores.

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 se activan por un proceso que requiere la utilización simultánea de 2 de 5 dispositivos criptográficos (tarjetas).

El acceso a la clave privada del Suscriptor se realiza por medio de un código de activación (PIN). El dispositivo tiene un sistema de protección contra intentos de acceso que lo bloquean cuando se introducen más de tres veces un código de acceso erróneo. Para desbloquear el dispositivo, el Suscriptor dispone de un código de desbloqueo (PUK). Si se introduce tres veces erróneamente, el dispositivo se bloquea definitivamente, quedando inservible.

El PIN y el PUK son secretos y personales para usuario y son entregados al Suscriptor por la RA en el proceso de emisión del certificado. Tanto el PIN como el PUK pueden ser modificados posteriormente por el usuario utilizando las aplicaciones correspondientes.

6.2.8. Método de desactivación de la clave privada

La clave privada del Suscriptor de certificados con DCCF quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de

lectura.

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, incluyendo también los dispositivos que contengan copias de dichas claves.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

La CA conservará todas las claves públicas durante el período exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación 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 o firmante 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 SIGNE 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 SIGNE detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.5.1. Requerimientos técnicos de seguridad específicos

Cada servidor de la CA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de CA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.

- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del Suscriptor y la CA y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- uto-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 SIGNE.

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.

6.2.2.7 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.

6.2.2.8 Gestión del sistema de acceso

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

a) Gestión general de la CA:

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

b) Generación del certificado:

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

- La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la CA.

c) Gestión de la revocación:
   - Las instalaciones de la CA están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregular al sistema de revocaciones.
   - La revocación se refiere a la pérdida de efectividad de un certificado digital de forma permanente. La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de CA.

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

6.6.2.9 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 catálogo de activos de Firmaprofesional, S.A.

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

Firmaprofesional realiza 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 encriptada.

6.8. Fuente de tiempo

El tiempo se obtiene mediante un hardware específico con reloj atómico de átomo de rubidio, sincronización GPS y consulta al Real Observatorio de la Armada[9], siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en el RFC 5905 “Network Time Protocol”.

[9] 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 5280 "Internet X.509 Public Key InfrastructureCertificate and CRL Profile"
- RFC 3739 “QualifiedCertificatesProfile”

El perfil común a todos los certificados es el siguiente:

Campo del certificado	Nombre	Descripción
Versión	Nº de versión	*V3 (versión del estándar X509)*
Serial	nº de serie	*Código único con respecto al nombre distinguido 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 Subject Alternative Name	-	email del Suscriptor (o de la CA)
X509v3 Issuer Alternative Name	-	URI: https://www.signe.es/signe-ac
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 Content Commitment 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
X509v3 Authority Key Identifier	-	id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma
X509v3 Authority Information Access	-	URI dónde se encuentra el certificado de la CA
X509v3 CRL Distribution Points	-	URI de la CRL
X509v3 Certificate Policies	-	OID de la política de certificación propia de SIGNE correspondiente al certificado. URI de la DPC User Notice : Nota de texto que se puede desplegar en la pantalla del usuario Cuando sea de aplicación, OID de la política europea. Cuando sea de aplicación, OID de la política española (de empleado público, de representante legal, etc).

QcStatements	-	Existen los siguientes tipos: Id-etsi-qcs-QcCompliance (a añadir cuando el certificado es reconocido) Id-etsi-qcs-QcSSCD (a añadir cuando la clave privada se guarda en un DCCF) id-etsi-qcs-QcLimitValue: Límite del valor de las transacciones Id-etsi-qcs-QcRetentionPeriod: Indica el periodo de retención de la documentación. Id-etsi-qcs-QcPDS: URI con documento PDS, obligatorio en lengua inglesa y opcional otras lenguas. Id-etsi-qcs-QcType: Indica el tipo de certificado: • id-etsi-qct-esign, es un certificado para crear firmas electrónicas • id-etsi-qct-eseal, es un certificado para crear sellos electrónicos • id-etsi-qct-web, es un certificado para la autenticación web

Las extensiones aquí presentadas corresponden con todas las que pueden contener los certificados emitidos. 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
1.2.840.113549.1.1.5	sha1withRSAencryption	OID del algoritmo de firma
1.2.840.113549.1.1.11	sha256withRSAencryption	OID del algoritmo de firma
1.2.840.113549.1.1.1	rsaEncryption	OID de Clave pública

SIGNE declara que las claves del firmante o suscriptor creadas por la CA son

generadas usando un algoritmo reconocido como apropiado para los usos identificados en esta CPS o en la correspondiente CP, durante el tiempo de validez del mismo.

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 Suscriptor, Adicionalmente, podrá contener un código numérico de identificación, o el NIF del Suscriptor, distinguiéndose el valor mediante la inclusión previa de una etiqueta "/ núm.:" o " – NIF ". Adicionalmente, podrá contener en algún tipo de certificado, indicaciones de uso "firma", "cifrado" o "autenticación".
E, E-mail	E-mail	Correo electrónico del Suscriptor
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF o NIE del Suscriptor
SN, surName	Apellidos	Apellidos del Suscriptor

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 emplean la codificación UTF8String para los campos que contengan caracteres especiales, y PrintableString para el resto.

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

El OID de la DPC es el siguiente: 1.3.6.1.4.1.36035.0.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 DPC y las PC.
- 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 SIGNE 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) de Firmaprofesional

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha2WithRSAEncryption
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 la autoridad de certificación SIGNE Autoridad de Certificación:

CAMPOS	VALORES
Versión	2
Número de CRL	Número incremental
Algoritmo de firma	Sha2WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	(fecha de emisión de la CRL, tiempo UTC)
fecha de próxima actualización	Fecha efectiva de emisión + 7 días
Identificador de la clave de autoridad	Hash de la clave del emisor
Sólo contiene Certificados de usuario	NO
Sólo contiene Certificados de la entidad emisora	NO
Lista de revocación de certificados (CRL) indirecta	NO
Entradas de la CRL	Nº de serie del certificado Fecha de revocación Código de razón

7.3. Perfil de OCSP

El Servicio de Validación de Certificados se basa en el uso del protocolo OCSP sobre HTTP, definido en la norma RFC 2560 “Online Certificate Status Protocol – OCSP”.

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

8. Auditorías de cumplimiento y otros controles

En el momento de inicio de actividad del prestador la autoridad de certificación SIGNE se encuentra en proceso de preparación para la obtención del sello WEBTRUST. Sin embargo, la creación de la CA, así como su mantenimiento y gestión se realizan bajo un entorno auditado y certificado con el sello WEBTRUST, bajo el control de Firmaprofesional.

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).

8.1. Frecuencia de las auditorías

Se realizarán auditorías periódicas, generalmente con carácter anual.

SIGNE se compromete a realizar las auditorías necesarias para obtener en su propio nombre dicha certificación.

8.2. Cualificación del auditor

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

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).

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 SIGNE.

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 DPC), así como la política de privacidad de la información y protección de datos personales y proporciona sus servicios en conformidad con dichas afirmaciones.

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

   - La información del Suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la CA), y
   - La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

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

   - La información de Suscriptores y usuarios está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio de la CA publicadas.
   - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.

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

8.4.1. Auditoría en las Autoridades de Registro

Las Autoridades de Registro que tengan acceso al software 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 SIGNE 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, SIGNE 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), SIGNE 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 SIGNE.

9. Aspectos 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 SIGNE.

9.1.2 Tarifas de acceso a la información de estado o revocación

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

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

9.1.2. Tarifas de otros servicios

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

9.2. Responsabilidades económicas

SIGNE, 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 igual o superior a 3.000.000 €.

9.3. Confidencialidad de la información

SIGNE 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.

SIGNE 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 DPC 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

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

9.3.3. Responsabilidad en la protección de información confidencial

Es responsabilidad de SIGNE 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, SIGNE 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	2102790784
Servicio de atención al público	Avda. de la Industria, 18 28760 Tres Cantos Madrid

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 de Firmaprofesional[10]:

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 y de SIGNE

f) Copias de seguridad y recuperación → Política de Seguridad FP y de SIGNE

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 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
	Titulaciones académicas (Titulación y organismo emisor)
Ámbito profesional	CIF correspondiente a la persona o entidad a la que está vinculado el Suscriptor
	Departamento o Unidad al que pertenezca el Suscriptor
	Cargo, titulo o rol del Suscriptor en la organización
	Ubicación geográfica del Suscriptor en la organización (empresa o colegio)
	Número de empleado 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 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..

9.4.5. 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 SIGNE, 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 solicita 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 y novedades a los usuarios registrados vía correo electrónico.

La información personal recabada de los usuarios registrados es almacenada en la base de datos propiedad SIGNE 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 SIGNE 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 SIGNE mediante comunicación escrita dirigida a:

SIGNE S.A.
Tratamiento de datos personales
Avenida de la Industria, 18
28760, Tres Cantos
Madrid

Cualquier rectificación y/o cancelación de los datos de carácter personal conllevará la revocación del certificado.

9.4.6. Revelación en el marco de un proceso judicial

Los datos de carácter personal podrán ser revelados por SIGNE 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

Propiedad de la DPC

- La propiedad intelectual de esta DPC y de las distintas PC pertenece a SIGNE, salvo las secciones donde explícitamente se atribuye su propiedad a Firmaprofesional.

Propiedad de los certificados

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

- SIGNE 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 SIGNE y la parte que reproduzca y/o distribuya el certificado, así como con las correspondientes condiciones generales de emisión.

Propiedad de las claves

- El par de claves es propiedad del Suscriptor.

9.6. Obligaciones

9.6.1. Obligaciones de la CA

SIGNE se obliga según lo dispuesto en este documento, así como lo dispuesto en la normativa sobre prestación de servicios de Certificación y la Ley 59/2003, y el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, principalmente a:

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

b) Publicar esta DPC, las CP y la PDS en su página Web.

c) Informar sobre las modificaciones de esta DPC 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:

f) Emitir certificados conforme a esta DPC y a los estándares de aplicación.

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

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

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

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

Sobre custodia de información:

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

l) No almacenar ni copiar los datos de creación de firma del Suscriptor, cuando

así lo disponga la normativa vigente.

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

n) Proteger sus claves privadas de forma segura.

o) 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 DPC para la emisión de certificados, principalmente a:

a) Respetar lo dispuesto en esta DPC y en la PC correspondiente al tipo de certificado que emita.

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

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

En el ciclo de vida de los certificados:

a) Comprobar la identidad de los Solicitantes de certificados según lo descrito en esta DPC o mediante otro procedimiento que haya sido aprobado por SIGNE.

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 SIGNE, de la DPC, la PDS y de la PC correspondiente al certificado.

d) Tramitar y entregar los certificados conforme a lo estipulado en esta DPC, la

PDS y en la PC correspondiente.

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

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

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

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

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

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 Suscriptores

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

a) Custodiar su clave privada y el DCCF (si la política exige su uso) de manera diligente.

b) Usar el certificado según lo establecido en la presente DPC.

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.

9.7. Exención de garantía

SIGNE 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

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

SIGNE 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 DPC o según otro procedimiento aprobado por SIGNE.

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. Limitación de responsabilidades

SIGNE 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 SIGNE 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 DPC, 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 SIGNE.

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 DPC 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 SIGNE 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.

9.10. Periodo de validez

9.10.1. Plazo

La DPC, la PDS y las distintas PC entran en vigor en el momento de su publicación.

9.10.2. Sustitución y derogación de la DPC

La presente DPC, la PDS y las distintas PC 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 DPC o PC 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

SIGNE 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 SIGNE https://www.signe.es/signe-ac para realizar cualquier tipo de notificación y comunicación.

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

9.12. Cambios en las especificaciones

9.12.1. Procedimiento para los cambios

9.12.1.1 Elementos que pueden cambiar sin necesidad de notificación

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

9.12.1.2 Cambios con notificación

Los elementos de esta DPC pueden ser cambiados unilateralmente por SIGNE sin preaviso. Las modificaciones pueden tener causa justificativa en motivos legales, técnicos o comerciales.

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

9.12.1.3 Mecanismo de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los Suscriptores, usuarios u terceros serán notificados inmediatamente a los interesados mediante la publicación en la Web de SIGNE.

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.

Los datos de contacto se encuentran en el apartado 1.6.2 Persona de contacto.

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.

Será responsabilidad de la autoridad de administración de las políticas (PA) decidir si se trata de un cambio menor o mayor de versión.

9.13. Reclamaciones y resolución de disputas

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

9.14. Normativa aplicable

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

- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- 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

SIGNE 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 PC correspondientes.

9.16.2. Independencia

La invalidez de una de las cláusulas contenidas en esta DPC 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.