Signe - Autoridad de Certificación

Declaración de Prácticas de Certificación

Documento:	SIGNE-ES-AC-DPC-01
Versión:	3.0
Fecha:	24/02/2021
Tipo de documento:	PÚBLICO

Historial de versiones

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
2.0	Adaptación a eIDAS	28/02/2018
2.1	Homogeneización de la terminología sobre los distintos soportes de los certificados.	31/07/2018
2.2	Sección 6.2.3: eliminación en la sección de párrafo sobre custodia de claves por parte del Suscriptor, ya que no se da el caso. Sección 9.14: se actualiza incluyendo el REGLAMENTO de Protección de datos	30/11/2018
2.3	Cambios en el formato. Adaptación a la normativa vigente de protección de datos en España. Homogeneización de la terminología de entidades participantes (Solicitante, Suscriptor, Firmante o Creador de sello, Custodio de claves). Añadido un tipo de certificados corporativos no cualificados (Certificados Corporativos de Firma Empresarial). Cambios en la validación del correo electrónico. Añadida la revocación por correo electrónico. Homogeneización en la generación y entrega de claves y certificados en soporte Otros dispositivos utilizando un dispositivo software. Aclaraciones en el método de activación de la clave privada en DCCF y DCCS centralizados. En los formatos de nombres de los perfiles de certificados, en los campos del DN comunes a todos los certificados de persona física: eliminación de campo E-mail, cambio en formato del valor del campo serialNumber, cambios en aclaraciones. Correcciones menores.	22/03/2019
2.4	Ajuste de la codificación del documento. Correcciones menores.	19/03/2020

3.0	Añadido etiquetado del tipo de documento. Adaptación a la Ley 6/2020. Cambio del certificado de la Autoridad de Certificación Subordinada de SIGNE. Añadido OID del certificado del Servicio OCSP. Añadida la autenticación de la identidad de una entidad sin personalidad jurídica y de una condición de autónomo o empresario individual. Añadidos en el soporte Otros dispositivos los tipos dispositivo criptográfico portable, dispositivo criptográfico centralizado y dispositivo externo. Añadidas nuevas circunstancias para la revocación. Añadida la solicitud de revocación de certificados por SIGNE, Firmaprofesional o una Autoridad de Registro, mediante procedimientos internos. Añadidos los requisitos de comprobación de revocación en línea por OCSP. Añadidos el hosting, la gestión y la operación de plataformas de la RA realizados directamente por SIGNE. Nuevo rol Administradores de Operadores RA y cambios en las incompatibilidades entre roles. Añadidas las acciones a realizar antes del del cese de actividad de una CA de SIGNE sin trasferencia de la gestión de los certificados emitidos a otro PSC. Cambios en el método de destrucción de la clave privada de la CA, para que no resulten afectadas el resto de claves gestionadas por el dispositivo criptográfico hardware (HSM). Se emplea la codificación UTF8String en todos los atributos de los DN de los certificados, contengan o no caracteres especiales, excepto en los atributos en los que es obligatorio utilizar la codificación PrintableString (C, Country; Serial Number). Añadido enlace para obtener información adicional sobre el tratamiento de datos personales obtenidos. Correcciones menores.	24/02/2021

Índice

1. Introducción

1.1. Presentación

Signe S.A. (en adelante SIGNE) es una sociedad 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 realiza su actividad como Prestador de Servicios de Confianza (PSC) para la emisión de certificados cualificados y no cualificados de firma electrónica y certificados cualificados de sello electrónico según el 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 (en adelante, "Reglamento eIDAS") y conforme a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, "Ley 6/2020"). En adelante, denominaremos a estos servicios prestados por SIGNE "servicios de certificación".

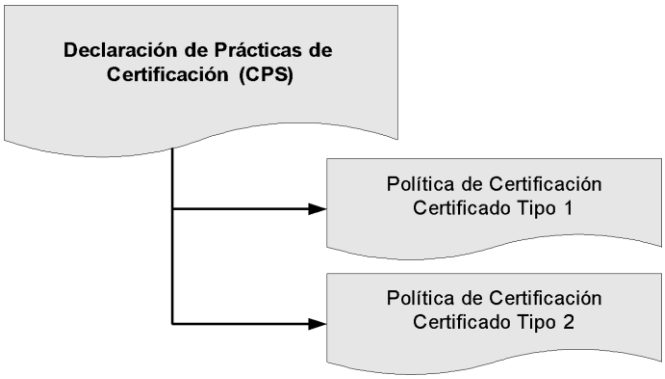
Los servicios de certificación prestados por SIGNE están orientados a los egresados, estudiantes que han completado sus estudios y se encuentran en situación de obtener el título que acredite la consecución de los mismos, y a Corporaciones Públicas y Privadas (como empresas, entidades privadas o públicas,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

Los detalles de la gestión de los certificados que emite un prestador de servicios de confianza 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. El presente documento constituye 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 de PKI (en inglés PDS o PKI Disclosure Statement), además de los requerimientos que se encuentran en la Política de Certificación (PC, en inglés CP o Certificate Policy).

Existe una política de certificación por cada tipo de certificado emitido y un texto de divulgación de PKI común a todos los tipos de certificados.



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

1.2. Nombre del documento e identificación

1.2.1. Identificación

Nombre	Declaración de Prácticas de Certificación
Código	SIGNE-ES-AC-DPC-01
Versión	3.0
Descripción	Declaración de Prácticas de Certificación de Signe S.A.
Fecha de emisión	24/02/2021
Tipo de documento	PÚBLICO
OID	1.3.6.1.4.1.36035.0.3.0
Localización	https://www.signe.es/signe-ac/dpc

1.2.2. OID

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: 0 = de Servicio (D = 1 = Servicio OCSP) 1 = de Titulado 2 = Corporativo de Persona Física 5 = Corporativo de Sello Electrónico 10 = de Sello de Órgano 20 = Corporativo de Firma Empresarial (no cualificado) D = Dispositivo: 1 = DCCF o DCCS portable / Nivel Alto 2 = Otros dispositivos / Nivel Medio 3 = DCCF o DCCS centralizado / Nivel Alto
2	*No usado actualmente*	*No usado actualmente*
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

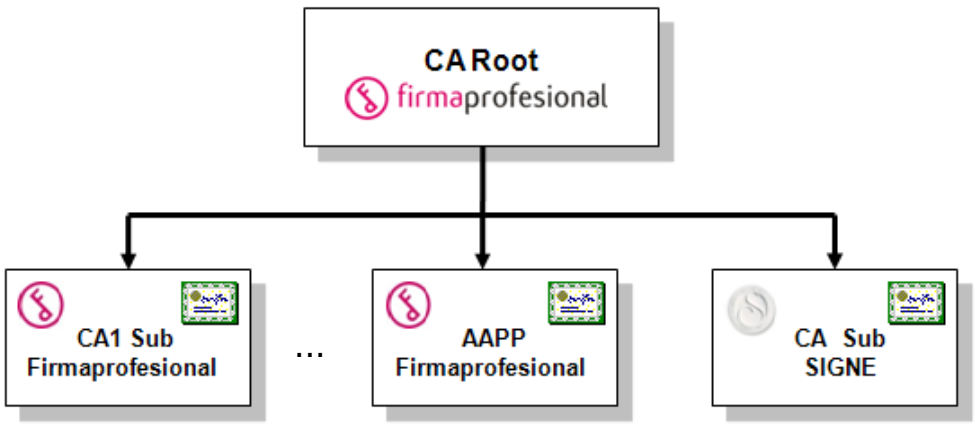
1.3.1. Prestador de Servicios de Confianza (PSC)

SIGNE es un Prestador de Servicios de Confianza (PSC) que emite certificados cualificados y no cualificados de firma electrónica y certificados cualificados de sello electrónico según el Reglamento Reglamento eIDAS y conforme a la Ley 6/2020.

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. Autoridades 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 CA pertenecientes a la Jerarquía de Certificación.

Se dispone de dos versiones del certificado de la Autoridad de Certificación Raíz, ambas con el mismo par de claves y los mismos datos de identificación, una generada con el algoritmo SHA1 y otra con el algoritmo SHA256:

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 2030

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 2036

Tipo de clave: RSA 4096 bits – SHA256

Autoridades de Certificación Subordinadas

Se denominan Autoridades de Certificación Subordinadas (CA Sub) 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.

SIGNE dispone de una Autoridad de Certificación Subordinada, con una única versión vigente de su certificado, generada con el algoritmo SHA256 y 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 DPC:

CN: ***SIGNE Autoridad de Certificacion - 2020***

Hash SHA1: 2B3 8EBE 17A8 B895 6810 ECE8 20A5 7188 1137 8653

Válido desde el 30 de julio de 2020 hasta el 31 de diciembre de 2030

Tipo de clave: RSA 4096 bits – SHA256

Restricciones técnicas (extKeyUsage):

Autenticación del cliente (clientAuth - 1.3.6.1.5.5.7.3.2)

Correo seguro (emailProtection - 1.3.6.1.5.5.7.3.4)

La Autoridad de Certificación Subordinada "**SIGNE Autoridad de Certificacion - 2020**" emite certificados digitales a personas físicas y a corporaciones privadas y públicas, conforme a lo establecido en el Reglamento eIDAS, en la Ley 6/2020 y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

En el presente documento, cuando se indique "la CA" sin especificar cuál, se entenderá que se refiere a la CA Subordinada de SIGNE.

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.
- Validar la identidad del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves, y comprobar que cumplen con los requisitos necesarios para la solicitud de los certificados.
- Validar los atributos de la persona física o jurídica que constarán en el certificado como Firmante o Creador del sello.
- Gestionar la generación de claves y la emisión del certificado.
- Hacer entrega del certificado al Firmante o al Custodio de claves.

Podrán actuar como RA de SIGNE:

- La propia SIGNE directamente.
- Cualquier Corporación que llegue a un acuerdo con SIGNE para la emisión de certificados a nombre de la Corporación o de aquellas personas físicas con las que la Corporación tenga una vinculación, ya sea como empleados, asociados, colaboradores, clientes o proveedores.
- 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 de SIGNE.

La entidad que actúe como RA de SIGNE podrá autorizar a una o varias personas como **Operadores de 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 correspondiente Política de Certificación.

1.3.5. Suscriptor

El Suscriptor es la persona física o jurídica o la entidad sin personalidad 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** y para la **Administración Pública**, el Suscriptor es siempre una Corporación (empresa privada, entidad pública, universidad) o una Administración Pública que ha contratado los servicios de certificación de SIGNE. En este caso, la Corporación o la Administración Pública es la propietaria del certificado.

1.3.6. Firmante o Creador del sello

De acuerdo con el Reglamento eIDAS, el Firmante es la persona física que crea la firma electrónica y el Creador del sello es la persona jurídica que crea el sello electrónico.

Los datos del Firmante constan en su certificado de firma electrónica. Los datos del Creador del sello constan en su certificado de sello electrónico.

Concretamente:

- En el caso de certificados **Personales, Corporativos de Persona Física** y **Corporativos de Firma Empresarial**, el Firmante es la persona física titular del certificado.
- En el caso de certificados **Corporativos de Sello Electrónico** y **de Sello de Administración, órgano o entidad de derecho público**, el Creador del sello es la Corporación (empresa privada, entidad pública, universidad) o la Administración Pública que ha contratado los servicios de certificación de SIGNE, es decir, el Suscriptor del certificado.

1.3.7. Custodio de claves

El Custodio de claves es la persona física que posee un dispositivo de creación de firma o sello o tiene control sobre el mismo, y que actúa en su nombre y derecho, o bien como sujeto vinculado a una Corporación (empresa, entidad privada o pública) o a una Administración Pública, organismo o entidad de derecho público, suscriptor del certificado.

El Custodio de claves será responsable de custodiar los datos de creación de firma electrónica o sello electrónico, es decir, la clave privada asociada al certificado, o los datos de acceso a los mismos, es decir, los datos que permiten utilizar la clave privada asociada al certificado.

Concretamente:

- En el caso de certificados **Personales, Corporativos de Persona Física** y **Corporativos de Firma Empresarial**, el Custodio de claves es siempre la persona física titular del certificado, es decir, el Firmante.
- En el caso de certificados **Corporativos de Sello Electrónico** y para la **Administración Pública**, el Custodio de claves es el Solicitante u otra persona física autorizada por el Solicitante para obtener el certificado.

1.3.8. 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 de la Autoridad de Certificación Raíz de Firmaprofesional está reconocido por por los principales fabricantes de software como Microsoft, la Fundación Mozilla, Apple o Adobe.

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 cualificados emitidos por SIGNE 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 el Reglamento eIDAS y en la Ley 6/2020.

Los terceros que confían en los certificados deberán tener presentes las limitaciones en su uso.

1.4. Tipos de certificados

1.4.1. Certificados Personales cualificados

Certificado de Titulado: son certificados cualificados de firma electrónica según el Reglamento eIDAS y conforme a la Ley 6/2020, que permiten identificar telemáticamente al Suscriptor/Firmante como poseedor de una determinada titulación académica.

Estos certificados son emitidos en Otros dispositivos[1], 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 POLÍTICAS DE CERTIFICADOS PERSONALES CUALIFICADOS	
1.3.6.1.4.1.36035.1.1.D	PC de Titulado

[1] Otros dispositivos diferentes de Dispositivo Cualificado de Creación de Firma (DCCF)

D = Dispositivo/Nivel de Seguridad:
2 = Otros dispositivos / Nivel Medio

1.4.2. Certificados Corporativos cualificados

Los certificados Corporativos cualificados son certificados cualificados de firma electrónica y de sello electrónico según el Reglamento eIDAS y conforme a la Ley 6/2020, cuyo Suscriptor es una Corporación (empresa, entidad privada o pública).

- **Certificados Corporativos de Persona Física**: son certificados cualificados de firma electrónica, 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 Electrónico**: son certificados cualificados de sello electrónico, emitidos a personas jurídicas de conformidad con el artículo 38 del Reglamento eIDAS.

OID DE POLÍTICAS DE CERTIFICADOS CORPORATIVOS CUALIFICADOS	
1.3.6.1.4.1.36035.1.2.D	PC Corporativo de Persona Física
1.3.6.1.4.1.36035.1.5.D	PC Corporativo de Sello Electrónico

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

1.4.3. Certificados Corporativos no cualificados

Los certificados Corporativos no cualificados son certificados no cualificados de firma electrónica según el Reglamento eIDAS y conforme a la Ley 6/2020, cuyo Suscriptor es una Corporación (empresa, entidad privada o pública).

- **Certificados Corporativos de Firma Empresarial**: son certificados electrónicos no cualificados de firma electrónica, que identifican al Suscriptor como Corporación y al Firmante como vinculado a esa Corporación, como su representante legal o voluntario (apoderado).

OID DE POLÍTICAS DE CERTIFICADOS CORPORATIVOS NO CUALIFICADOS	
1.3.6.1.4.1.36035.1.20.D	PC Corporativo de Firma Empresarial

D = Dispositivo/Nivel de Seguridad:
2 = Otros dispositivos / Nivel Medio

1.4.4. Certificados para la Administración Pública cualificados

Los Certificados para la Administración Pública son certificados electrónicos emitidos de acuerdo con la LRJSP.

- **Certificados de Sello de Administración, órgano o entidad de derecho público:** son certificados cualificados de sello electrónico, para dispositivos informáticos, programas o aplicaciones dedicados a firmar en nombre de la Administración, órgano o entidad de derecho público en sistemas de firma electrónica para la actuación administrativa automatizada. Son certificados acordes con el Anexo III del Reglamento eIDAS y el artículo 40 de la LRJSP.

OID DE POLÍTICAS DE CERTIFICADOS PARA LA ADMINISTRACIÓN PÚBLICA CUALIFICADOS	
1.3.6.1.4.1.36035.1.10.D	PC Sello de Órgano

D = Dispositivo/Nivel de Seguridad:
1 = DCCS portable / Nivel Alto, 3 = DCCS 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 certificados revocados.

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 Administración de las políticas

1.6.1. Organización responsable

El Departamento Técnico de SIGNE es la organización responsable de la administración de esta DPC y de las PC.

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:	+34 918 06 00 99
Dirección:	SIGNE S.A. Avda. de la Industria, 18 28760 Tres Cantos (Madrid)

1.6.3. Frecuencia de revisión

Esta DPC y las PC serán revisadas y si procede, actualizadas, anualmente.

1.6.4. Procedimiento de aprobación

Esta DPC y las PC son aprobadas por el Comité de Sistemas de Gestión de SIGNE antes de ser publicadas, después de que se controlen las versiones de las mismas, a fin de evitar modificaciones y suplantaciones no autorizadas y el uso de documentación obsoleta.

Las nuevas versiones aprobadas de esta DPC y de las PC serán enviadas al organismo de supervisión y publicadas en la página web de SIGNE https://www.signe.es/signe-ac/dpc. Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

1.7. Definiciones y siglas

1.7.1. Definiciones

Servicios de Confianza: el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y

certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;

Servicio de Confianza Cualificado: un servicio de confianza que cumple los requisitos aplicables establecidos en el Reglamento eIDAS.

Prestador de Servicios de Confianza: persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.

Prestador Cualificado de Servicios de Confianza: prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación.

Firmante: una persona física que crea una firma electrónica.

Firma Electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el Firmante para firmar.

Firma Electrónica Avanzada: la firma electrónica que cumple los siguientes requisitos contemplados en el artículo 26 del Reglamento eIDAS:

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Firma Electrónica Cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

Certificado de Firma Electrónica: una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.

Certificado Cualificado de Firma Electrónica: un certificado de firma electrónica que ha

sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento eIDAS.

Creador de un Sello: una persona jurídica que crea un sello electrónico.

Sello Electrónico: datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

Sello Electrónico Avanzado: un sello electrónico que cumple los siguientes requisitos contemplados en el artículo 36 del Reglamento eIDAS:

a) Estar vinculado al creador del sello de manera única;

b) permitir la identificación del creador del sello;

c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y

d) d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Sello electrónico Cualificado: un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

Clave Pública y Clave Privada: par de claves de criptografía asimétrica en la que se basa la PKI, de forma 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 clave se la denomina privada y únicamente es utilizada por el titular del certificado.

Datos de Creación de la Firma Electrónica (Clave Privada): los datos únicos que utiliza el Firmante para crear una firma electrónica.

Datos de creación del sello electrónico (Clave Privada): los datos únicos que utiliza el creador del sello electrónico para crearlo

Datos de Validación (Clave Pública): los datos utilizados para validar una firma electrónica o un sello electrónico.

Dispositivo de Creación de Firma Electrónica: un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

Dispositivo de Creación de Sello Electrónico: un equipo o programa informático

configurado que se utiliza para crear un sello electrónico.

Dispositivo Cualificado de Creación de Firma (DCCF): un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II del Reglamento eIDAS.

Dispositivo Cualificado de Creación de Sello (DCCS): un dispositivo de creación de sellos electrónicos que cumple *mutatis mutandis* los requisitos enumerados en el anexo II del Reglamento eIDAS.

Sello de Tiempo Electrónico: datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

Sello Cualificado de Tiempo Electrónico: un sello de tiempo electrónico que cumple los requisitos establecidos en artículo 42 del Reglamento eIDAS.

Función Hash: 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.

Lista de Certificados Revocados: lista donde figuran la relación de certificados revocados.

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

Autoridad de Certificación: entidad de confianza, responsable que emite y revoca certificados.

Autoridad de Registro: entidad responsable de identificar y autenticar a los solicitantes, a los titulares y a los responsables de los certificados.

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. Siglas

ARL:	Lista de Certificados de CA Revocados (Authority Revocation List)
CA:	Autoridad de Certificación (Certification Authority)
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
DCCF:	Dispositivo Cualificado de Creación de Firma
DCCS:	Dispositivo Cualificado de Creación de Sello

DN:	Nombre distinguido (Distinguished Name)
DPC:	Declaración de Prácticas de Certificación (Certificate Practice Statement)
HSM:	Módulo de seguridad hardware criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
OID:	Identificador de objeto único (Object identifier)
PDS	Texto de Divulgación (PKI Disclosure Statement)
PC:	Política de Certificación (Certificate Policy)
PKI:	Infraestructura de Clave Pública (Public Key Infrastructure)
PSC:	Prestador de Servicios de Confianza (Trust Service Provider)
RA:	Autoridad de Registro (Registration Authority)
TSA:	Autoridad de sellado de tiempo (Time Stamp Authority)
VA	Autoridad de validación (Validation Authority)

Estándares y Organismos de estandarización

CEN:	Comité Europeo de Normalización
CWA:	CEN Workshop Agreement
ETSI:	European Telecommunications Standard Institute
FIPS:	Federal Information Processing Standard
IETF:	Internet Engineering Task Force
PKIX:	Grupo de trabajo del IETF sobre PKI
PKCS:	Public Key Cryptography Standards
RFC:	Request For Comments

2. Repositorios y publicación de información

2.1. Repositorios

Acceso	Descripción	URL
Público	DPC, Políticas de Certificación y PDS	https://www.signe.es/signe-ac/dpc http://www.signe.es/signe-ac/dpc
Público	Certificado CA Raíz Firmaprofesional	https://www.signe.es/signe-ac/crl/caroot.crt http://www.signe.es/signe-ac/crl/caroot.crt https://crl.firmaprofesional.com/caroot.crt http://crl.firmaprofesional.com/caroot.crt
Público	Certificado CA Subordinada SIGNE	https://www.signe.es/signe-ac/crl/signe2020.crt http://www.signe.es/signe-ac/crl/signe2020.crt
Público	ARL: Lista de Certificados de CA Revocados (CRL emitida por CA Raíz Fimaprofesional)	https://www.signe.es/signe-ac/crl/fproot.crl http://www.signe.es/signe-ac/crl/fproot.crl https://crl.firmaprofesional.com/fproot.crl http://crl.firmaprofesional.com/fproot.crl
Público	CRL: Lista de Certificados de entidad final Revocados (CRL emitida por CA Subordinada SIGNE)	https://www.signe.es/signe-ac/crl/signe2020.crl http//www.signe.es/signe-ac/crl/signe2020.crl
Público	Servicio de Validación de Certificados de CA (OCSP de CA Raíz Fimaprofesional)	https://ocsp.firmaprofesional.com http://ocsp.firmaprofesional.com
Público	Servicio de Validación de Certificados de entidad final (OCSP de CA Subordinada SIGNE)	https://servicios.signe.es/ocsp http://servicios.signe.es/ocsp

Los repositorios están referenciados por la URL. Cualquier cambio en las URL 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 (PDS) 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 PC que correspondan de SIGNE publicadas en su página web https://www.signe.es/signe-ac/dpc.

2.2.3. Difusión de los certificados

El Firmante o el Creador del sello 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 electrónica o un sello electrónico. Este envío se realizará generalmente de manera automática, adjuntando el certificado a todo documento firmado o sellado electrónicamente.

2.3. Frecuencia de publicación

Según la Declaración de Prácticas de Certificación de Firmaprofesional, la CA Raíz emitirá y publicará una **Lista de Certificados de CA Revocados (ARL)** como mínimo cada seis meses, o extraordinariamente, cuando se produzca la revocación de un certificado de Autoridad de Certificación Subordinada.

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

SIGNE publicará 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, los certificados de CA y las listas de certificados revocados se publicarán en repositorios de acceso público sin control de acceso.

Los certificados emitidos podrían ser publicados en repositorios públicos, siempre que el Suscriptor o el Firmante del certificado consienta de forma expresa esta acción.

Los servicios de validación por el protocolo OCSP son de acceso público sin control de acceso y gratuitos.

3. Identificación y Autenticación

3.1. Registro de Nombres

3.1.1. Tipos de nombres

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

- ETSI EN 319 412 conocida como “European profiles for Qualified Certificates”
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",
- RFC 3739 “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”.

3.1.2. Necesidad de que los nombres sean significativos

Los atributos del DN del certificado referentes al nombre y apellidos de persona física se corresponderán con los datos del Firmante (certificado de firma electrónica) o, en su caso, del Custodio de claves (certificado de sello electrónico, si contiene los datos de identidad del Custodio de claves) que consten en el documento de identificación presentado.

Los atributos del DN referentes a la denominación o razón social de persona jurídica, de entidad sin personalidad jurídica, o de autónomo o empresario individual se corresponderán con los datos del Suscriptor que consten en los registros oficiales.

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 (certificado de prueba), y que no cumple todo lo especificado en la presente DPC y en la PC correspondiente.

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, así como por la RFC 5280.

3.1.5. Unicidad de los nombres

El nombre distinguido (DN) de los certificados emitidos será único para cada Suscriptor y/o Firmante. Los atributos del DN que contienen el código identificativo del Suscriptor y/o el código identificativo del Firmante se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

3.1.6. Reconocimiento, autenticación y papel de las marcas registradas

La CA no asume compromisos en la emisión de certificados respecto al uso por los Suscriptores de una marca comercial. 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 Cualificado portable o centralizado, o en Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado, o dispositivo software, 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 Firmante o Creador de sello.

Cada RA es responsable de garantizar la entrega del dispositivo al Firmante o al Custodio de claves de forma segura.

En los otros casos (certificado en Otros dispositivos del tipo dispositivo externo), el método de prueba de la posesión de la clave privada por el Custodio de claves será la entrega de una petición PKCS #10 que contiene la correspondiente clave pública.

3.2.2. Autenticación de la identidad de una persona jurídica

La Autoridad de Registro realizará la identificación y autenticación de la persona jurídica identificada en el certificado de sello electrónico (Suscriptor) o, en su caso, de la persona jurídica identificada en el certificado de firma electrónica (Suscriptor), conforme a los siguientes puntos:

1. La RA verificará los siguientes datos de la persona jurídica (Suscriptor):

    - Denominación o razón social.
    - Número de identificación fiscal (NIF) o código equivalente utilizado en el país a cuya

legislación esté sujeto el Suscriptor.
- Los datos relativos a la constitución y personalidad jurídica.
- Los datos relativos a la extensión y vigencia de las facultades de representación del Solicitante.

2. La RA podrá verificar los datos indicados en el punto 1 según uno de los siguientes procedimientos:

   - Mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible.

   - Mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos (por ejemplo, un acceso en línea al Registro Mercantil).

   La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos indicados en el punto 1.

3. El Solicitante deberá firmar la solicitud del certificado, declarando que sus datos de identidad y los datos de la persona jurídica incluidos en la misma son correctos.

   Si la solicitud del certificado ha sido firmada electrónicamente con un certificado cualificado de firma electrónica vigente que permita verificar los datos indicados en el punto 1 y su inscripción en el correspondiente registro público si así resulta exigible (certificado cualificado de firma electrónica con atributo de representante):

   - En el caso de un certificado de firma electrónica que identifica a una persona física (Firmante) como vinculada a la persona jurídica (Suscriptor), no se exigirá lo indicado en el punto 2.

   - En el caso de un certificado de sello electrónico, de acuerdo con el artículo 24.1.c) del Reglamento eIDAS, no se exigirá lo indicado en el punto 2 si para la expedición del certificado cualificado de firma electrónica con atributo de representante se ha identificado a su Firmante mediante su personación ante un Operador de RA conforme a lo especificado en el apartado 3.2.3.

La RA registrará los datos y documentos relativos a la identificación y autenticación de la persona jurídica identificada en el certificado de sello electrónico o, en su caso, de la persona jurídica identificada en el certificado firma electrónica.

3.2.3. Autenticación de la identidad de una persona física

La Autoridad de Registro realizará la identificación y autenticación de la persona física

identificada en el certificado de firma electrónica (Firmante) o de la persona física Solicitante del certificado de sello electrónico, conforme a los siguientes puntos:

1. La identificación de la persona física exigirá su personación ante un Operador de RA y se acreditará mediante el Documento Nacional de Identidad, el pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física si su firma en la solicitud del certificado ha sido legitimada en presencia notarial.

2. En el caso de un certificado de firma electrónica que contenga otros atributos de la persona física (Firmante), éstos deberán comprobarse mediante los documentos oficiales que los acrediten.

   La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos indicados.

3. Lo dispuesto en los puntos anteriores podrá no ser exigible en los siguientes casos:

   a) De acuerdo con el artículo 7.6 de la Ley 6/2020, cuando la identidad u otros atributos permanentes de la persona física constaran ya a SIGNE o a la RA en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubiese empleado el medio señalado en el punto 1 y el período de tiempo transcurrido desde la identificación fuese menor de cinco años. En este caso:

      - No se exigirá lo indicado el punto 1, si los datos de identidad de la persona física a registrar constaran ya a SIGNE o a la RA.

      - No se exigirá lo indicado en el punto 2 para aquellos atributos permanentes que constaran ya a SIGNE o a la RA, pero se exigirá para aquellos atributos permanentes que no constaran a SIGNE o a la RA, y para aquellos atributos no permanentes que constaran o no a SIGNE o a la RA.

   b) De acuerdo con el artículo 24.1.c) del Reglamento eIDAS, cuando para solicitar un certificado se utilice un certificado cualificado de firma electrónica vigente para cuya expedición se hubiera identificado a la persona física en la forma prescrita en el punto 1. En este caso:

      - No se exigirá lo indicado el punto 1, si los datos de identidad de la persona física a registrar están contenidos en el certificado utilizado.

      - No se exigirá lo indicado en el punto 2 para aquellos atributos, permanentes o no, contenidos en ambos certificados (el utilizado y el solicitado), pero sí se exigirá para aquellos atributos, permanentes o no, contenidos en el certificado solicitado y no contenidos en el certificado utilizado.

4. La persona física deberá firmar la solicitud del certificado, declarando que sus datos de identidad y, en su caso, otros atributos personales incluidos en la misma son correctos.

   Si la solicitud del certificado ha sido firmada electrónicamente con un certificado cualificado de firma electrónica vigente, se tendrá en cuenta lo indicado en el punto

3.b).

5. En el caso de un certificado de firma electrónica que identifica a la persona física (Firmante) como vinculada a una persona jurídica, a una entidad sin personalidad jurídica o a un autónomo o empresario individual (Suscriptor), el Solicitante deberá firmar una autorización para que el Firmante pueda obtener el certificado.

   La autorización deberá contener, al menos, los siguientes datos del Firmante que estarán contenidos en el certificado: Nombre y apellidos, Código identificativo, Cargo, título o rol en la organización y Dirección de correo electrónico.

   La autorización puede contener otros atributos del Firmante que estarán contenidos en el certificado, pudiendo utilizarse, en su caso, como documento oficial para la comprobación de los mismos, conforme a lo indicado en el punto 2.

La Autoridad de Registro realizará la identificación y autenticación de la persona física Solicitante del certificado de firma electrónica, en el caso de que sea distinta al Firmante, o de la persona física Custodio de claves del certificado de sello electrónico, en el caso de que sea distinta al Solicitante, conforme a los siguientes puntos:

1. La identificación de la persona física se acreditará mediante una copia del Documento Nacional de Identidad, el pasaporte u otros medios admitidos en Derecho.

2. La persona física deberá firmar la solicitud del certificado, declarando que sus datos de identidad incluidos en la misma son correctos.

   Si la solicitud del certificado ha sido firmada electrónicamente con un certificado cualificado de firma electrónica vigente con los mismos datos de identidad que los incluidos en la solicitud, no se exigirá lo indicado en el punto 1.

3. En el caso de un certificado de sello electrónico, el Solicitante deberá firmar una autorización para que la persona física (Custodio de claves) pueda obtener el certificado.

   La autorización deberá contener, al menos, los siguientes datos del Custodio de claves que, dependiendo del tipo del certificado, podrán o no estar contenidos en el certificado: Nombre y apellidos, Código identificativo, Cargo en la organización y Dirección de correo electrónico.

La RA registrará los datos y documentos relativos a la identificación y autenticación del Solicitante y del Firmante del certificado de firma electrónica, o del Solicitante y del Custodio de claves del certificado de sello electrónico.

3.2.4. Autenticación de la identidad de una entidad sin personalidad jurídica

En su caso, la Autoridad de Registro realizará la identificación y autenticación de la entidad sin personalidad jurídica identificada en el certificado de firma electrónica (Suscriptor),

conforme a los siguientes puntos:

1. La RA verificará los siguientes datos de la entidad sin personalidad jurídica (Suscriptor):

   - Denominación o razón social, tal como se recoja en los registros oficiales, si resulta exigible su inscripción en los mismos, en el país a cuya legislación esté sujeto el Suscriptor.
   - Número de identificación fiscal (NIF) o, en su defecto, otro código identificativo de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales, si resulta exigible su inscripción en los mismos, en el país a cuya legislación esté sujeto el Suscriptor.
   - Los datos relativos a la constitución.
   - Los datos relativos a la extensión y vigencia de las facultades de representación del Solicitante.

2. La RA podrá verificar los datos indicados en el punto 1 según uno de los siguientes procedimientos:

   - Mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro oficial si así resulta exigible.

   - Mediante consulta en el registro oficial en el que, en su caso, estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros oficiales.

   La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos indicados en el punto 1.

3. El Solicitante deberá firmar la solicitud del certificado, declarando que sus datos de identidad y los datos de la entidad sin personalidad jurídica incluidos en la misma son correctos.

   Si la solicitud del certificado ha sido firmada electrónicamente con un certificado cualificado de firma electrónica vigente que permita verificar los datos indicados en el punto 1 y su inscripción en el correspondiente registro oficial si así resulta exigible (certificado cualificado de firma electrónica con atributo de representante), no se exigirá lo indicado en el punto 2.

La RA registrará los datos y documentos relativos a la identificación y autenticación de la entidad sin personalidad jurídica identificada en el certificado de firma electrónica.

3.2.5. Autenticación de la identidad de una condición de autónomo o empresario individual

En su caso, la Autoridad de Registro realizará la identificación y autenticación de la condición de autónomo o empresario individual identificada en el certificado de firma electrónica (Suscriptor), conforme a los siguientes puntos:

1. La RA verificará los siguientes datos de la condición de autónomo o empresario individual (Suscriptor):

   - Denominación o razón social que consta en el certificado (nombre y apellidos y/o nombre comercial de su establecimiento y, opcionalmente, código CNAE o IAE o código equivalente en otro país), tal como se recoja en los registros oficiales en el país a cuya legislación esté sujeto el Suscriptor.
   - Número de identificación fiscal (NIF) o código equivalente utilizado en el país a cuya legislación esté sujeto.
   - Los datos relativos al alta de autónomo o empresario individual en la Agencia Tributaria y/o en la Seguridad Social, o en los organismos que correspondan en el país a cuya legislación esté sujeto el Suscriptor.
   - Los datos relativos a la vigencia del alta de autónomo o empresario individual.

2. La RA podrá verificar los datos indicados en el punto 1 según uno de los siguientes procedimientos:

   - Mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro oficial si así resulta exigible.

   - Mediante consulta en el registro oficial en el que estén inscritos los datos indicados en el punto 1, pudiendo emplear los medios telemáticos facilitados por los citados registros oficiales.

   La RA se reserva el derecho de no aprobar la solicitud del certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos indicados en el punto 1.

3. El Solicitante deberá firmar la solicitud del certificado, declarando que sus datos de identidad y los datos relativos a su condición de autónomo o empresario individual en la misma son correctos.

   Si la solicitud del certificado ha sido firmada electrónicamente con un certificado cualificado de firma electrónica vigente que permita verificar los datos indicados en el punto 1 y su inscripción en el correspondiente registro oficial si así resulta exigible, no se exigirá lo indicado en el punto 2.

La RA registrará los datos y documentos relativos a la identificación y autenticación de la condición de autónomo o empresario individual identificada en el certificado de firma

electrónica.

3.2.6. 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 parte.
- 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 RA. La RA deberá enviar a SIGNE la documentación correspondiente al nuevo operador, así como su autorización para que actúe como Operador de RA.
    - Asegurar que los Operadores de RA hayan recibido formación suficiente para el desempeño de sus funciones.

3.2.7. Validación del correo electrónico

Las direcciones de correo electrónico incluidas en los certificados y, en su caso, las de los Custodios de claves son validadas siempre por el Solicitante y, en su caso, también por el Firmante o por el Custodio de claves, mediante su inclusión en las respectivas solicitudes del certificado firmadas por el Solicitante, y por el Firmante o por el Custodio de claves y, en su caso, en la autorización firmada por el Solicitante.

3.3. Identificación y autenticación para solicitudes de renovación

3.3.1. Renovación de certificados online

Para los tipos de certificados que recojan en su Política de Certificación la renovación de certificados online, el Firmante se podrá identificar y autenticar en el proceso de renovación online utilizando su anterior certificado si éste cumple lo siguiente:

- Para su emisión, se ha identificado al Firmante mediante su personación ante un Operador de RA conforme a lo especificado en el apartado 3.2.3.
- Está vigente (no ha caducado, ni ha sido revocado).
- Quedan menos de 45 días para que caduque.

3.3.2. Renovación de certificados ante un Operador de RA

La RA realizará la identificación y autenticación del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves del mismo modo que en la validación inicial de la identidad, conforme a lo especificado en los apartados 3.2.1 y 3.2.2, en su caso, en los apartados 3.2.3 y 3.2.4, y en la Política de Certificación correspondiente.

3.4. Identificación y autenticación para solicitudes de revocación

La identificación y autenticación del Suscriptor, o del Firmante o del Custodio de claves para una solicitud de revocación de un certificado podrá ser realizada por:

a) El propio Suscriptor, o el Firmante o el Custodio de claves, para los tipos de certificados que recojan en su Política de Certificación la revocación de certificados online, mediante el uso de su código identificativo y el código de revocación proporcionado durante el proceso de emisión del certificado.

b) Los operadores autorizados de SIGNE (Responsables de Revocación), mediante los procedimientos que el operador considere oportunos.

La identificación y autenticación de cualquier persona distinta al Suscriptor, o al Firmante o al Custodio de claves para una solicitud de revocación de un certificado será realizada por los operadores autorizados de SIGNE (Responsables de Revocación), mediante los procedimientos que el operador considere oportunos.

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, con participación, en su caso, del Firmante (certificado de firma electrónica) o del Custodio de claves (certificado de sello electrónico). Los requisitos que debe reunir un Solicitante, un Firmante y un Custodio de claves 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, y el Firmante o el Custodio de claves deberán ponerse en contacto con una RA de SIGNE para gestionar la solicitud del certificado.

La RA proporcionará al Solicitante, y al Firmante o al Custodio de claves la siguiente información:

- Documentación necesaria a presentar para la tramitación de su solicitud y para verificar la identidad del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves.
- 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.

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, del Solicitante, y del Firmante o del Custodio de claves. Este proceso deberá ser realizado previamente a la emisión del certificado, conforme a lo especificado en los apartados 3.2.1 y 3.2.2, en su caso, en los apartados 3.2.3 y 3.2.4, y en la Política de Certificación correspondiente.

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, y el Firmante o el Custodio de claves, incluyendo la validación de la identidad del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves.

Si la información no fuese correcta, la RA deberá denegar la petición, contactando con el Solicitante, y el Firmante o el Custodio de claves para comunicarles el motivo.

Si la información 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 y para la Administración Pública, SIGNE verificará que el instrumento jurídico existe y que ha sido firmado, siendo responsabilidad del Solicitante verificar el cargo, título o rol declarado del Firmante o del Custodio de claves en la Corporación o en la Administración Pública, así como, en su caso, su vinculación con la misma.

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 Firmante o al Custodio de claves.

- Para los certificados en Dispositivos Cualificados de Creación de Firma o Sello (DCCF, DCCS) portable o centralizado, en Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado:
    - En el caso de DCCF o DCCS o dispositivo criptográfico portable, la RA le hará entrega al Firmante o al Custodio de claves o verificará que éste posee un DCCF o DCCS o dispositivo criptográfico portable homologado por SIGNE (en el caso de DCCF o DCCS, deberá cumplir los requisitos establecidos en el Anexo II del Reglamento eIDAS).
    - Activación del dispositivo: en el caso que el Firmante o el Custodio de claves 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 en el dispositivo utilizando el sistema proporcionado por la RA.
- Para los certificados en Otros dispositivos del tipo dispositivo software:

  - Se proporcionará un código de autenticación al Firmante o al Custodio de claves que deberá presentar para proceder con la descarga del certificado (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá).

- Para los certificados en Otros dispositivos del tipo dispositivo externo:

  - El par de claves habrá sido generado previamente en un dispositivo externo gestionado por el Suscriptor y/o el Custodio de claves.

  - El Custodio de claves entregará a la RA la clave pública en una petición de certificado en formato PKCS #10.

- En todos los 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 PKCS#10 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 Firmante o del Custodio de claves.

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

4.3.2. Notificación al Firmante o al Custodio de claves de la emisión del certificado

La RA notificará al Firmante o al Custodio de claves 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 al Firmante o al Custodio de claves, ya sea personal o telemáticamente.

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

4.4.2. Publicación del certificado

Una vez que el certificado haya sido emitido y haya sido aceptado por el Firmante o por el Custodio de claves, el certificado podría ser publicado en los repositorios de certificados que se consideren necesarios, siempre que el Suscriptor, o el Firmante o el Custodio de claves no se hayan 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 de PKI (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, 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

SIGNE Autoridad de Certificación enviará una notificación de recordatorio de caducidad del certificado por correo electrónico al Firmante (certificado de firma electrónica) o al Suscriptor (certificado de sello electrónico) 45 días, 30 días y 15 días antes de la fecha de caducidad del certificado.

Existen dos posibilidades para la renovación de certificados:

a) Proceso de renovación ante un Operador de RA, que se efectuará del mismo modo que la emisión de un certificado.

b) Proceso de renovación online, permitida sólo para los tipos de certificado que lo recojan en su Política de Certificación, que se detalla a continuación.

4.7.1. Circunstancias para la renovación online

Solamente se podrá proceder a la renovación online del certificado si ésta se permite para el tipo de certificado y si, además, se cumplen las condiciones siguientes en el certificado actual:

- Para su emisión, se ha identificado al Firmante mediante su personación ante un Operador de RA conforme a lo especificado en el apartado 3.2.3.
- Está vigente (no ha caducado, ni ha sido revocado).
- Quedan menos de 45 días para que caduque.

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

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

4.7.3. Tramitación de las peticiones de renovación online

Se realizarán los siguientes pasos:

- Se notificará al Firmante por correo electrónico que puede renovar su certificado.
- El Firmante deberá acceder a una página web de renovación de su certificado.
- Mediante el uso de su certificado a renovar, el Firmante deberá autenticarse y firmar la renovación de su certificado (en su caso, incluye la firma del Contrato de Prestación de Servicios de Certificación).
- Se procederá a la generación del nuevo par de claves.
- Se enviará por un canal seguro la clave pública a la CA en formato PKCS #10 u otro equivalente.
- Seguidamente se realizará la generación del certificado mediante un procedimiento que utilizará protección contra falsificación y mantendrá la confidencialidad de los datos intercambiados.
- El certificado generado será entregado al Firmante.

El nuevo certificado contendrá los mismos datos del Firmante y, en su caso, del Suscriptor que el anterior certificado.

4.7.4. Notificación de la emisión del certificado renovado

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

4.7.5. Forma de aceptación del certificado renovado

El certificado se aceptará al firmar electrónicamente la renovación.

4.7.6. Publicación del certificado renovado

Una vez el certificado haya sido renovado, el nuevo certificado podría ser publicado en los repositorios de certificados que se consideren necesarios reemplazando al certificado anterior, siempre que el Suscriptor o 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. Circunstancias para la revocación

Un certificado podrá ser revocado debido a las siguientes causas:

a) Circunstancias que afectan a la información contenida en el certificado:
   - Descubrimiento de que alguno de los datos contenidos en la solicitud del certificado y que constan en él es falso o incorrecto.
   - Alteración posterior de alguna de las circunstancias verificadas para la expedición del certificado y que constan en él, por ejemplo, pérdida o cambio de la vinculación del Firmante con la Corporación que consta en el certificado.
   - Modificación de cualquier dato contenido en el certificado.
   - Extinción de la personalidad jurídica, o disolución de la entidad sin personalidad jurídica, o baja de autónomo o empresario individual, de la Corporación que consta en el certificado.

b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:
   - Compromiso o sospecha de 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 privada o del certificado.
   - Acceso o utilización no autorizados por un tercero de la clave privada del certificado.
   - El incumplimiento por parte del Suscriptor, o del Firmante o del Custodio de claves de las normas de uso del certificado expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre la CA, la RA y el Suscriptor.
   - En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de la clave privada o el certificado no cumple los estándares de seguridad mínimos necesarios para garantizar su seguridad.

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 dispositivo criptográfico.
   - Incumplimiento por parte del Suscriptor, o del Firmante o del Custodio de claves de las normas de uso del dispositivo criptográfico expuestas en la presente DPC, en la PC correspondiente o en el instrumento jurídico vinculante entre la CA, la RA y el Suscriptor.

d) Circunstancias que afectan al Suscriptor, al Solicitante, o al Firmante o al Custodio de claves:
   - 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 Firmante.
   - Oposición o modificación, por parte del Solicitante, o del Firmante o del Custodio de claves, de los datos contenidos en el fichero de datos de carácter personal de SIGNE.
   - Infracción por el Solicitante del certificado de los requisitos y obligaciones establecidos para la solicitud del mismo.
   - Infracción por el Suscriptor, o por el Firmante o por el Custodio de claves de sus obligaciones y responsabilidades establecidas en la presente DPC, en la PC correspondiente o en el instrumento jurídico correspondiente vinculante entre la CA, la RA y el Suscriptor.
   - Capacidad modificada judicialmente o incapacidad sobrevenida, total o parcial, o fallecimiento del Firmante.

- Solicitud formulada por el Firmante o el Suscriptor o un tercero autorizado.

e) Otras circunstancias:
   - Resolución judicial o administrativa que lo ordene.
   - Cese de la actividad de la CA, salvo que la gestión de los certificados electrónicos emitidos sea transferida a otro PSC (revocación masiva de todos los certificados vigentes emitidos por la CA).
   - Cese de la actividad de una RA, salvo que expresamente se decida lo contrario (revocación masiva de todos de los certificados vigentes emitidos por esa RA).
   - Cualquier otra causa lícita especificada en la presente DPC o en la PC correspondiente.

4.9.2. Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

a) El propio Suscriptor, o el Firmante o el Custodio de claves, que deberán solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

b) SIGNE, Firmaprofesional o una Autoridad de Registro, que deberán solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

c) Cualquier otra 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:

- El propio Suscriptor, o el Firmante o el Custodio de claves, en los casos de revocación de certificados online.

- Los operadores autorizados de SIGNE (Responsables de Revocación).

Adicionalmente, los operadores autorizados de la CA (Operadores de CA - Operadores de Certificación) podrán tramitar la revocación masiva de certificados por cese de actividad de la CA o de una RA.

En todo caso, al tiempo de revocarse el certificado, se enviará un comunicado al Firmante (certificado de firma electrónica) o al Suscriptor (certificado de sello electrónico), especificando la fecha y la hora y el motivo de la revocación.

4.9.3. Procedimientos de solicitud de revocación

Existen distintas alternativas para solicitar la revocación de un certificado.

4.9.3.1. Procedimiento online

Para los tipos de certificados que recojan en su Política de Certificación la revocación de certificados online, SIGNE pondrá a disposición del Suscriptor, y/o del Firmante o del Custodio de claves un formulario web desde el que podrá solicitar y tramitar la revocación de su certificado.

Mediante el formulario, SIGNE solicitará al Suscriptor, o al Firmante o al Custodio de claves:

- Su código identificativo.
- El código de revocación proporcionado durante el proceso de emisión del certificado.
- Aceptar explícitamente la tramitación de la solicitud de revocación y las consecuencias de ésta.

4.9.3.2. Procedimientos internos

SIGNE, Firmaprofesional y las Autoridades de Registro solicitarán la revocación de un certificado mediante procedimientos internos.

Un operador autorizado de SIGNE (Responsable de Revocación) atenderá la solicitud de revocación en horario de oficina[2].

El operador deberá identificar y autenticar al solicitante de la revocación mediante los procedimientos que considere oportunos, y comprobar que la causa comunicada se corresponde con alguna de las circunstancias anteriormente indicadas.

Una vez correctamente identificado el solicitante de la revocación y comprobada la causa comunicada, el operador procederá a tramitar la revocación.

El tiempo máximo entre la recepción de la solicitud por el operador y su decisión de tramitar o no la revocación será de 23 horas y 45 minutos.

4.9.3.3. Revocación telefónica

SIGNE dispone de un servicio de revocación telefónico en el que se podrá solicitar la revocación de un certificado:

[2] Días laborables en Madrid de lunes a viernes, de 8:30 a 18:30

Servicio de revocación telefónico (horario de oficina[3]): 902 30 17 01

Alternativamente, se podrá solicitar la revocación de un certificado telefónicamente a la RA en la que se tramitó la correspondiente solicitud del certificado, y dicha RA derivará la solicitud a SIGNE.

Un operador autorizado de SIGNE (Responsable de Revocación) atenderá la solicitud de revocación en horario de oficina.

El operador deberá identificar y autenticar al solicitante de la revocación mediante los procedimientos que considere oportunos, y comprobar que la causa comunicada se corresponde con alguna de las circunstancias anteriormente indicadas.

Además, en el caso de que la revocación del certificado sea solicitada por una persona distinta al Suscriptor, o al Firmante o al Custodio de claves, el operador deberá verificar la causa de revocación comunicada mediante los procedimientos que considere oportunos.

Una vez correctamente identificado el solicitante de la revocación y comprobada y, en su caso, verificada la causa comunicada, el operador procederá a tramitar la revocación.

El tiempo máximo entre la recepción de la solicitud por el operador y su decisión de tramitar o no la revocación será de 23 horas y 45 minutos.

4.9.3.4. Revocación por correo electrónico

SIGNE dispone de un servicio de revocación por correo electrónico en el que se podrá solicitar la revocación de un certificado:

Servicio de revocación por correo electrónico: signe-ac@signe.com

Alternativamente, se podrá solicitar la revocación de un certificado por correo electrónico a la RA en la que se tramitó la correspondiente solicitud del certificado, y dicha RA derivará la solicitud a la RA de SIGNE.

Un operador autorizado de SIGNE (Responsable de Revocación) atenderá la solicitud de revocación en horario de oficina[4].

El operador deberá identificar y autenticar al solicitante de la revocación mediante los procedimientos que considere oportunos, y comprobar que la causa comunicada se corresponde con alguna de las circunstancias anteriormente indicadas.

[3] Días laborables en Madrid de lunes a viernes, de 8:30 a 18:30

[4] Días laborables en Madrid de lunes a viernes, de 8:30 a 18:30

Además, en el caso de que la revocación del certificado sea solicitada por una persona distinta al Suscriptor, o al Firmante o al Custodio de claves, el operador deberá verificar la causa de revocación comunicada mediante los procedimientos que considere oportunos, y comprobar que se corresponde con alguna de las circunstancias anteriormente indicadas.

Una vez correctamente identificado el solicitante de la revocación y comprobada y, en su caso, verificada la causa de revocación comunicada, el operador procederá a tramitar la revocación.

El tiempo máximo entre la recepción de la solicitud por el operador y su decisión de tramitar o no la revocación será de 23 horas y 45 minutos.

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

Una vez que la revocación haya sido debidamente tramitada en la RA, la revocación se hará efectiva inmediatamente.

4.9.5. Obligación de verificación de las revocaciones por los terceros que confían en los certificados

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

4.9.6. Frecuencia de emisión de las CRL

La CRL de los certificados de CA (ARL) se emite antes de que hayan transcurrido 180 días desde la emisión de la anterior CRL (antes de su fin de validez), o lo antes posible después de que se produzca una revocación (proceso manual).

La CRL de los certificados de entidad final se emite cada 24 horas, o a más tardar 10 minutos después de que se produzca una revocación, con una validez de 7 días (proceso automático).

4.9.7. Tiempo máximo entre la generación y la publicación de las CRL

Una vez emitida la CRL de los certificados de CA (ARL), ésta se publica lo antes posible (proceso manual).

Una vez emitida la CRL de los certificados de entidad final, ésta se publica a más tardar 5 minutos después (proceso automático).

4.9.8. Disponibilidad de sistemas en línea de verificación del estado de los certificados

SIGNE tiene disponibles dos sistemas en línea de verificación del estado de los certificados, uno mediante comprobación de revocación por CRL y otro por OCSP, ambos gratuitos y sin restricciones de acceso.

Las direcciones de acceso a ambos sistemas se encuentran en el apartado 2.1, así como en los certificados, en sus extensiones CRL Distribution Points y Authority Information Access.

4.9.9. Requisitos de comprobación de revocación en línea

Para el uso del sistema de comprobación de revocación en línea por CRL, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar el estado de revocación del certificado de entidad final en la última CRL emitida por la CA Subordinada de SIGNE, que podrá descargarse en la dirección URL contenida en el propio certificado, en su extensión CRL Distribution Points.
- Adicionalmente, se deberá comprobar el estado de revocación del certificado de la CA Subordinada de SIGNE en la última CRL emitida por la CA Raíz de Firmaprofesional (ARL), que podrá descargarse en la dirección URL contenida en el propio certificado, en su extensión CRL Distribution Points.
- Se deberá comprobar que cada CRL esté vigente (con un valor del campo *nextUpdate* posterior a la fecha y hora actuales) y firmada por la CA que ha emitido el certificado que se quiere validar.
- La información proporcionada en la última CRL emitida por la CA Subordinada de SIGNE se actualiza, como máximo, 15 minutos después de cada revocación (proceso automático).
- La información proporcionada en la última CRL emitida por la CA Raíz de Firmaprofesional (ARL) se actualiza, como máximo, 24 horas después de cada revocación (proceso manual).
- La información de cada certificado revocado en las CRL incluirá el correspondiente motivo de revocación conforme a la RFC 5280, excepto cuando el motivo de revocación sea *unspecified (0)*.
- Los certificados revocados que expiren son retirados de las CRL, excepto en el caso de la última CRL emitida por la CA Subordinada de SIGNE después de realizar una revocación masiva de todos los certificados vigentes emitidos, por el cese de actividad de la CA sin trasferencia de la gestión de los certificados emitidos a otro PSC.

Para el uso del sistema de comprobación de revocación en línea por OCSP, se debe

considerar lo siguiente:

- Se deberá comprobar el estado de revocación del certificado de entidad final en el servicio OCSP de la CA Subordinada de SIGNE, cuya dirección URL de acceso está contenida en el propio certificado, en su extensión Authority Information Access.

- Adicionalmente, se deberá comprobar el estado de revocación del certificado de la CA Subordinada de SIGNE en el servicio OCSP de la CA Raíz de Firmaprofesional, cuya dirección URL de acceso está contenida en el propio certificado, en su extensión Authority Information Access.

- Se podrá comprobar el estado de revocación de los certificados en los servicios OCSP utilizando los métodos GET o POST.

- Se deberá comprobar que cada respuesta OCSP esté vigente (con un valor del campo *nextUpdate* posterior a la fecha y hora actuales) y firmada con un certificado vigente (no expirado) emitido por la CA que ha emitido el certificado que se quiere validar, y que incluya las extensiones Key Usage con los usos *digitalSignature* y/o *nonRepudiation* y Extended Key Usage con el uso *OCSPSigning*.

- Se podrá comprobar el estado de revocación del certificado usado para firmar cada respuesta OCSP en la última CRL emitida por la CA que ha emitido dicho certificado, que podrá descargarse en la dirección URL contenida en el propio certificado, en su extensión CRL Distribution Points. Esta comprobación será opcional en el caso de que el certificado contenga la extensión *ocsp-nocheck*, y obligatoria en el caso de que el certificado no contenga esta extensión.

- La información proporcionada a través del servicio OCSP de la CA Subordinada de SIGNE se actualiza cada 5 minutos (proceso automático).

- La información proporcionada a través del servicio OCSP de la CA Raíz de Firmaprofesional se actualiza, como máximo, 24 horas después de cada revocación (proceso manual).

- La información de cada certificado revocado proporcionada a través de los servicios OCSP incluirá el correspondiente motivo de revocación conforme a la RFC 5280, excepto cuando el motivo de revocación sea *unspecified (0)*.

- La información proporcionada a través de los servicios OCSP se mantiene una vez que han expirado los certificados cuyo estado de revocación se consulta. Es decir, si se comprueba el estado de revocación de un certificado revocado después de que haya expirado, el servicio OCSP seguirá respondiendo que está revocado, así como la fecha y hora y el motivo de la revocación.

- No se podrá usar el servicio OCSP de la CA Subordinada de SIGNE en el caso de que ésta haya emitido una última CRL después de realizar una revocación masiva de todos los certificados vigentes emitidos, por el cese de actividad de la CA sin trasferencia de la gestión de los certificados emitidos a otro PSC.

4.10. Servicios de información del estado de certificados

4.10.1. Características operativas

SIGNE ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL), sin restricciones de acceso, en las direcciones indicadas en el apartado 2.1, así como en los certificados, en su extensión CRL Distribution Points.

SIGNE ofrece un servicio gratuito de validación de certificados por medio del protocolo OCSP, sin restricciones de acceso, en la dirección indicada en el apartado 2.1, así como en los certificados, en su extensión Authority Information Access.

Adicionalmente, SIGNE puede ofrecer otros 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 SIGNE, éste realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

En el caso del cese de actividad de la CA de SIGNE sin trasferencia de la gestión de los certificados emitidos a otro PSC, se realizará una revocación masiva de todos los certificados vigentes emitidos y se emitirá y publicará una última CRL que tendrá un valor del campo *nextUpdate* igual a la fecha y hora UTC 31/12/9999 23:59:59 y contendrá todos los certificados revocados, incluyendo aquéllos que hubiesen expirado y la extensión X.509 ExpiredCertsOnCRL. Esta última CRL de la CA de SIGNE estará disponible durante al menos 15 años desde su emisión, mientras que el servicio OCSP de la CA de SIGNE dejará de estar disponible.

La provisión de la información sobre el estado de los certificados queda garantizada en el caso de cese de la actividad de SIGNE como CA, mediante la transferencia de la gestión de los certificados emitidos a otro PSC, quien conservará la información relativa a los servicios de certificación prestados hasta entonces por SIGNE, o mediante la comunicación a la administración competente de la información relativa a todos los certificados cualificados expedidos cuya vigencia habrá sido extinguida, para que se haga cargo de su custodia.

4.10.3. Características adicionales

Se podrá consultar la información sobre el estado de los certificados, no sólo hasta que éstos expiren, sino más allá de dicha fecha, a través del servicio OCSP o, en el caso el cese

de actividad de la CA de SIGNE sin trasferencia de la gestión de los certificados emitidos a otro PSC, a través de la última CRL emitida por la CA de SIGNE.

SIGNE puede disponer de servicios avanzados de validación de certificados que requieran 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 la operación de las plataformas de las CA y de algunas plataformas de las RA de sus servicios de certificación. Con ello, SIGNE se adhiere a la Declaración de Prácticas de Certificación de Firmaprofesional, concretamente a su apartado 5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS) de Firmaprofesional, S.A., en la versión vigente en el momento de la publicación del presente documento.

El hosting, la gestión y la operación del resto de plataformas de las RA son realizados directamente por SIGNE.

5.1. Controles físicos

Firmaprofesional y SIGNE tienen 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 emisión 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 PSC.

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.

5.1.1. Ubicación física y construcción

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

La sala donde se realizan las operaciones criptográficas de las CA 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.

La sala donde se encuentran ubicadas las plataformas de las RA gestionadas por SIGNE posee 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 donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

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

Las instalaciones de las plataformas de las CA 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 de las plataformas de las CA 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.

El acceso a las salas de las plataformas de las RA gestionadas por SIGNE se realiza con lectores de tarjeta de identificación.

5.1.3. Alimentación eléctrica y aire acondicionado

Las instalaciones 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

En las instalaciones de las plataformas de las CA, 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.

En las instalaciones de las plataformas de las RA gestionadas por SIGNE, los sistemas de los servidores se ejecutan mediante el despliegue de un entorno virtualizado en alta disponibilidad, soportado sobre dispositivos redundantes de computación, almacenamiento de alto rendimiento y redes independientes de producción, gestión y almacenamiento.

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, mediante su destrucción física o haciendo ilegible la información contenida.

5.1.8. Copias de seguridad fuera de las instalaciones

Las plataformas de las CA y las plataformas de las RA gestionadas por SIGNE mantienen un almacén externo seguro para la custodia de documentos en papel, y de dispositivos y documentos electrónicos independiente del centro de datos.

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 garantizan 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.

Se establecen los siguientes roles de confianza, conforme a lo especificado en las normas ETSI EN 319 401 y ETSI EN 319 411-1:

- Responsable de Seguridad (*Security Officers*): mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad.
- Operadores de RA (*Registration Officers*): responsables de verificar la información necesaria para emitir los certificados y de aprobar las solicitudes de certificados.
- Responsables de Revocación (*Revocation Officers*): responsables de realizar los cambios en el estado de un certificado.
- Administradores del Sistema de Certificación (*System Administrators*): autorizado para instalar, configurar y mantener los sistemas para la administración de los servicios.
- Operadores de Sistemas (*System Operators*): responsables de operar día a día los sistemas. Autorizados para realizar backup de los sistemas.
- Auditores Internos (*System Auditors*): autorizados para ver los *logs* de los sistemas.

Adicionalmente, se establecen los siguientes roles de confianza específicos de las plataformas de las CA y las RA:

- Operadores de CA - Operadores de Certificación: responsables de activar las claves de la CA en el entorno Online, o de los procesos de firma de certificados y CRL en el entorno Root Offline.
- Administradores de Operadores RA: responsables de realizar las funciones de dar de alta a los operadores en las plataformas de las RA.

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

5.2.3. Identificación y autenticación por rol

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

Se establecen las siguientes incompatibilidades entre los roles establecidos en el apartado 5.2.1, de forma que una persona no pueda tener dos roles incompatibles:

- El rol Responsable de Seguridad (*Security Officer*) es incompatible con cualquier otro rol.
- Los roles de Operadores de RA (*Registration Officers*) y Responsables de Revocación (*Revocation Officers*) son incompatibles con los roles de Administradores del Sistema de Certificación (*System Administrators*), Operadores de Sistemas (*System Operators*) y Operadores de CA - Operadores de 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 dos meses trabajando en SIGNE, en Firmaprofesional o en la Entidad que asume funciones de RA con una relación laboral indefinida.

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.

SIGNE se asegura que los Operadores de RA son personal confiable de SIGNE o de la Entidad que asume funciones de RA.

El Operador de RA habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las solicitudes de certificados. Al final de dicho curso, SIGNE o un tercero designado por SIGNE procederá a evaluar sus conocimientos de los procedimientos relativos a la emisión de certificados por la CA de SIGNE, para asegurar la correcta realización de las tareas asignadas a su rol.

Tanto Firmaprofesional como SIGNE retirarán de sus funciones de confianza a un empleado

cuando tengan 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 para realizar funciones de confianza.

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

5.3.3. Requerimientos de formación

Firmaprofesional y SIGNE realizan los cursos necesarios a sus empleados y a los Operadores de 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 de formación al personal al menos cuando se realicen modificaciones en las tareas asignadas a un rol que así lo requieran, o cuando lo solicite alguna persona.

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 los requerimientos operacionales empleados por el PSC. 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 pondrán a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

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

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

Firmaprofesional y/o SIGNE registran y guardan los *logs* de todos los eventos relativos al sistema de seguridad de las CA y las RA. 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 o las RA 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 las CA.
- Encendido y apagado de las aplicaciones de las CA y las RA.
- Cambios en los detalles de las CA y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida de los certificados.
- Eventos asociados al uso del módulo criptográfico de la CA.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente, Firmaprofesional, SIGNE y las RA registran:

- 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

Firmaprofesonal y/o SIGNE conservan, 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 las CA y las RA.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del Solicitante, y del Firmante o del Custodio de Claves, 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 (plataformas de las CA) o trimestralmente (plataformas de la RA gestionadas por SIGNE) 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 al menos 15 años (en el caso de eventos del ciclo de vida de los certificados, desde el momento de la revocación o expiración del certificado) para garantizar la seguridad del sistema.

5.4.4. Protección de los registros de auditoría

Los *logs* de los sistemas son protegidos de su manipulación mediante mecanismos que aseguran su integridad.

En el caso de las plataformas de las CA, los *logs* son almacenados en dispositivos ignífugos.

En el caso de las plataformas de las CA, se protege la disponibilidad de los logs mediante el almacén en instalaciones externas al centro de datos.

Los dispositivos son manejados en todo momento por personal autorizado.

5.4.5. Procedimientos de respaldo de los registros de auditoría

Firmaprofesional y SIGNE disponen 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.

En el caso de las plataformas de las CA, se 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

En el caso de las plataformas de las CA, se realiza periódicamente una revisión de discrepancias en la información de los *logs* y actividades sospechosas, así como análisis de vulnerabilidades de direcciones IP internas y externas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

En el caso de las plataformas de la RA de SIGNE, se realiza periódicamente una revisión de vulnerabilidades y test de intrusión. Después, se analizarán y se corregirán las vulnerabilidades que se crea que son un riesgo.

5.5. Archivo de registros

5.5.1. Tipos de registros archivados

Se conservarán los datos del sistema que tengan lugar durante el ciclo de vida del certificado, incluyendo su renovación. Se almacenarán por Firmaprofesional y/o SIGNE o, por delegación de ésta, por la RA:

- Todos los registros de auditoría (*logs*).
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores, y cualquier información relativa a la identificación y autenticación de los Suscriptores, de los Solicitantes, y de los Firmantes o de los Custodios de claves, y a la solicitud, aceptación y entrega de los certificados.
- Solicitudes de emisión y revocación de certificados.
- Todos los certificados emitidos.
- CRL emitidas o registros del estado de los certificados generados (consultas OCSP).

Firmaprofesional y SIGNE son responsables 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 al menos 15 años desde el momento de la revocación o expiración del certificado. En particular:

- Los certificados se conservarán durante al menos 15 años desde su revocación o expiración.
- Los contratos con los Suscriptores, y cualquier información relativa a la identificación y autenticación de los Suscriptores, de los Solicitantes, y de los Firmantes o de los Custodios de claves, y a la solicitud, aceptación y entrega de los certificados serán conservados durante al menos 15 años desde el momento de la revocación o expiración del certificado.
- En el caso del cese de actividad de la CA de SIGNE sin trasferencia de la gestión de los certificados emitidos a otro PSC, se conservará la última CRL emitida por la CA de SIGNE, después de realizar una revocación masiva de todos los certificados vigentes emitidos, durante al menos 15 años desde su emisión.

5.5.3. Protección del archivo

Firmaprofesional y SIGNE aseguran la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas y/o instalaciones externas, en los casos en que así se requiera.

Además, se disponen de documentos técnicos 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

Firmaprofesional y SIGNE disponen 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 (interno o externo)

El sistema de archivo de la información de auditoría de la ECD es interno, si bien tanto Firmaprofesional como SIGNE disponen de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos.

5.5.7. Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos contra manipulaciones no autorizadas.

Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para obtener y llevar a cabo verificaciones de integridad de dichos archivos.

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 mientras existan certificados activos emitidos por la CA antigua. Se generará una nueva CA con una clave privada nueva.

El certificado de la nueva CA y su ARL se publicarán en los repositorios de SIGNE y Firmaprofesional en URL distintas a las de antigua CA.

5.6.2. CA Subordinada de SIGNE

En el caso de la CA Subordinada de SIGNE, se podrá optar por la renovación del certificado con o sin cambio de claves. Sólo cuando se realice el cambio de claves será aplicable lo descrito en el apartado anterior.

El certificado de la nueva CA y su CRL se publicarán en los repositorios de SIGNE en URL distintas a las de antigua CA.

5.7. Plan de recuperación de desastres

5.7.1. Procedimientos de gestión de incidentes y vulnerabilidades

Firmaprofesional y SIGNE han desarrollado un plan de contingencias, detallado en procedimientos documentados, 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 recursos hardware, software y/o datos, Firmaprofesional y/o SIGNE procederán de acuerdo con procedimientos documentados.

5.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de la Autoridad de Certificación

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

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

- Notificará al organismo de supervisión nacional en un plazo de 24 horas tras tener conocimiento del compromiso.
- Informará del compromiso de la clave privada de la CA a todos los Suscriptores y Firmantes, así como a otros clientes y otras CA o entidades con los cuales tenga acuerdos u otro tipo de relación, 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.
- Cesará la actividad de la CA sin trasferir la gestión de los certificados emitidos a otro PSC, pero pudiendo sustituir la CA por una nueva CA de SIGNE (cambio de claves de la CA).

5.7.4. Continuidad del negocio después de un desastre

La CA restablecerá los servicios críticos (revocación y publicación de información del estado

de los certificados) 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.

5.8. Cese de actividad

5.8.1. Autoridad de Certificación

Antes del cese de su actividad como CA, 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 del cese de su actividad como CA a todos los Suscriptores y Firmantes, así como a otros clientes y otras CA o entidades con los cuales tenga acuerdos u otro tipo de relación, con una antelación mínima de 2 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de RA de SIGNE en el procedimiento de emisión de certificados.
- De acuerdo con el artículo 9.3.c) de la Ley 6/2020, SIGNE podrá transferir, una vez acreditada la ausencia de oposición de los Suscriptores y Firmantes, la gestión de los certificados emitidos que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador cualificado, quien conservará la información relativa a los servicios de certificación prestados hasta entonces por SIGNE a efectos de lo previsto en el artículo 9.3.a) de la Ley 6/2020, o, en caso contrario, SIGNE extinguirá su vigencia mediante revocación.
- Comunicará a la administración competente, con una antelación mínima de tres meses, el cese de su actividad como CA y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién.
- En su caso, con carácter previo al cese definitivo de la actividad de SIGNE como CA sin trasferencia de la gestión de los certificados emitidos a otro PSC, comunicará a la administración competente la información relativa a los certificados cualificados expedidos cuya vigencia habrá sido extinguida, para que se haga cargo de su custodia a efectos de lo previsto en el artículo 9.3.a) de la Ley 6/2020.
- Comunicará a la administración competente, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra SIGNE, así como cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad como CA.
- SIGNE indica en su plan de finalización del servicio qué información será retornada.

Antes del cese de actividad de una CA de SIGNE sin trasferencia de la gestión de los certificados emitidos a otro PSC, SIGNE, con la colaboración de Firmaprofesional, realizará las siguientes acciones en el orden indicado:

1. En el caso de que el cese de actividad de la CA sea debido a su sustitución por una nueva CA de SIGNE (cambio de claves de la CA), informar a los Suscriptores, ofreciéndoles la posibilidad de reemitir sus certificados con la nueva CA.
2. Revocar todos los certificados vigentes firmados con la clave privada de la CA (revocación masiva).
3. Emitir y publicar una última CRL firmada con la clave privada de la CA, que tendrá un valor del campo *nextUpdate* igual a la fecha y hora UTC 31/12/9999 23:59:59 y contendrá todos los certificados revocados firmados con la clave privada de la CA, incluyendo aquéllos que hubiesen expirado y la extensión X.509 ExpiredCertsOnCRL.
4. Revocar todos los certificados de la CA vigentes que contienen la clave pública asociada a la clave privada de la CA, e informar de dicha revocación a la administración competente.
5. Destruir la clave privada de la CA.

5.8.2. Autoridad de Registro

Ante el cese de actividad de una Autoridad de Registro de un colectivo específico, SIGNE:

- Dejará de emitir y renovar certificados desde esa RA.
- Revocará los certificados de operador vigentes de esa RA.
- Revocará todos los certificados vigentes 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 o electrónico, a SIGNE.

6. Controles de seguridad técnica

SIGNE subcontrata a Firmaprofesional el hosting, la gestión y la operación de las plataformas de las CA y de algunas plataformas de las RA de sus servicios de certificación. Con ello, SIGNE se adhiere a la Declaración de Prácticas de Certificación de Firmaprofesional, concretamente a su apartado 6. CONTROLES DE SEGURIDAD TÉCNICA del documento DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN de Firmaprofesional, S.A., en la versión vigente en el momento de la entrada en vigor del presente documento.

El hosting, la gestión y la operación del resto de plataformas de las RA son realizados directamente por SIGNE.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

La generación de las claves de la CA Raíz de Firmaprofesional y la CA Subordinada de SIGNE se realiza, de acuerdo con un procedimiento documentado de ceremonia de claves, dentro de una sala de seguridad, en un dispositivo criptográfico hardware (HSM), por personal autorizado según los roles de confianza con un control dual, y en presencia de testigos[5] y un auditor externo.

Firmaprofesional y SIGNE garantizan que las claves de firma de la CA Raíz de Firmaprofesional y la CA Subordinada de SIGNE no son empleadas para otro supuesto que los indicados en este documento.

Para los certificados de los Suscriptores:

- En Dispositivo Cualificado de Creación de Firma o Sello (DCCF, DCCS) portable o centralizado, en Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado:
    - El par de claves será generado 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 de firma electrónica o sello electrónico (clave privada) y los datos de validación (clave pública).
- En Otros dispositivos del tipo dispositivo software:
    - El Firmante o el Custodio de claves recibirá por correo electrónico la

[5] Para ambas CA, al menos una persona con un cargo de relevancia en Firmaprofesional. Para la CA Subordinada de SIGNE, al menos una persona con un cargo de relevancia en SIGNE, a no ser que SIGNE decline su participación.

confirmación de la solicitud, juntamente con un código de autenticación a la aplicación online de emisión de certificados.

- Para poder acceder a la aplicación online de emisión de certificados, será necesario que el Firmante o el Custodio de claves proporcione el código de autenticación recibido.

- Una vez autenticado, el Firmante o el Custodio de claves procederá a la descarga del certificado electrónico (incluye la generación del par de claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo habrá establecido).

- En Otros dispositivos del tipo dispositivo externo:

  - El par de claves habrá sido generado previamente en un dispositivo externo gestionado por el Suscriptor y/o el Custodio de claves.

  - El Custodio de claves entregará a la RA la clave pública en una petición de certificado en formato PKCS #10.

6.1.2. Entrega de la clave privada

- En Dispositivo Cualificado de Creación de Firma o Sello (DCCF, DCCS) portable o centralizado, en Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado:

  - La clave privada será entregada junto al certificado en el DCCF o DCCS o dispositivo criptográfico portable. En los casos DCCF o DCCS o dispositivo criptográfico centralizado, no se entrega la clave privada.

  - La RA será responsable de garantizar la entrega del dispositivo portable al Firmante o al Custodio de claves, asegurándose así que éste último está en posesión de los datos de creación de firma electrónica o sello electrónico (clave privada) correspondientes a los datos de validación (clave pública) que constan en el certificado.

  - El dispositivo portable utiliza unos datos 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 y el dispositivo portable se enviarán al lugar de entrega por separado.

- En Otros dispositivos del tipo dispositivo software:

  - La descarga del certificado por el Firmante o por el Custodio de claves incluye la descarga de la clave privada, protegidos ambos con una contraseña que él mismo establecerá.

  - El Custodio de claves podrá instalar las claves y el certificado en su ordenador o sistema informático introduciendo la contraseña que él mismo estableció en el

momento de la descarga.

- En Otros dispositivos del tipo dispositivo externo:
    - No se entrega la clave privada porque está en un dispositivo externo gestionado por el Suscriptor y/o el Custodio de claves.

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 autofirmado preferiblemente en formato PKCS #10, 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

Los certificados de la CA Raíz de Firmaprofesional y la CA Subordinada de SIGNE y su fingerprint (huella digital) están 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 Subordinada SIGNE	4096	10
OCSP	2048	1
Suscriptores	2048	3 (máximo)
Operadores	2048	3 (máximo)

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

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

Concretamente los parámetros utilizados son los siguientes:

Signature suite	Hash function	Signature algorithm
sha256-with-rsa	SHA-256	RSA-PKCSv1_5

6.1.7. Usos admitidos de la clave (campo *Key Usage* de X.509 v3)

Todos los certificados emitidos por la CA de SIGNE incluyen las extensiones Key Usage y Extended Key Usage, indicando los usos habilitados de las claves.

Los usos admitidos para los certificados de la CA Raíz y la CA Subordinada de SIGNE son firma de certificados y firma de CRL.

Los usos admitidos de la clave para cada tipo de certificado de Suscriptores 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 Firmantes y Creadores de sellos de certificados cualificados en DCCF o DCCS portable son generadas de forma segura en 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 o en el artículo 51.1 del Reglamento eIDAS.

SIGNE verifica que los DCCF o DCCS portables utilizados, tanto si los aporta SIGNE como si los aportan los Firmantes o los Custodios de claves, 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 la CA Raíz y la CA Subordinada de SIGNE 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 en 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.

La clave privada de la CA Subordinada de SIGNE está custodiada en dispositivos criptográficos hardware certificados con la norma FIPS 140-2 nivel 3.

SIGNE no custodia copias de respaldo de las claves privadas de los Firmantes o Creadores de sellos de los certificados (key escrow).

6.2.4. Copia de seguridad de la clave privada

Existen unos dispositivos que permiten la restauración de las claves privadas de la CA Raíz y la CA Subordinada de SIGNE, que son almacenados de forma segura y sólo accesibles por personal autorizado, usando al menos un control dual en un medio físico seguro.

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

6.2.5. Archivo de la clave privada

La CA Raíz y la CA Subordinada de SIGNE no archivarán la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

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

Las claves privadas de la CA Raíz y la CA Subordinada de SIGNE se pueden transferir a o desde un módulo criptográfico por un proceso que requiere la utilización de 2 de 5 dispositivos criptográficos (tarjetas).

6.2.7. Almacenamiento de la clave privada en un módulo criptográfico

Existen documentos de ceremonia de claves de la CA Raíz y la CA Subordinada de SIGNE donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

6.2.8. Método de activación de la clave privada

- La clave privada de la CA Raíz se activa por un proceso que requiere la utilización de 2 de 4 dispositivos criptográficos (tarjetas), los cuales, junto a sus respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.
- La clave privada de la CA Subordinada de SIGNE se activan por un proceso que requiere la utilización de 1 de 4 dispositivos criptográficos (tarjetas), los cuales, junto a sus

respectivos PIN, constituyen, por tanto, los datos de activación de la clave privada.

- El acceso a la clave privada del Firmante o Creador del sello en DCCF o DCCS portable o en Otros dispositivos del tipo dispositivo criptográfico portable se realiza por medio de un código de activación (PIN).

  El dispositivo tiene un sistema de protección contra intentos de acceso que lo bloquea cuando se introduce más de un determinado número de veces un código erróneo. Para desbloquear el dispositivo, habitualmente, el dispositivo dispone de un código de desbloqueo (PUK). Si se introduce un determinado número de veces erróneamente el código de desbloqueo, el dispositivo se bloquea definitivamente, quedando inservible.

  Este PIN y este PUK constituyen, por tanto, los datos de activación de la clave privada.

  El PIN y el PUK son secretos y personales para el usuario y, en el caso de que el Firmante o el Custodio de claves no aporte su propio DCCF o DCCS o dispositivo criptográfico portable, le son entregados 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.

- El acceso a la clave privada del Firmante en DCCF centralizado se realiza mediante la utilización de dos factores de autenticación de categorías distintas, una contraseña definida por el Firmante, como factor de autenticación basado en el conocimiento, y una contraseña de un solo uso que el Firmante recibe en su teléfono móvil, como factor de autenticación basado en la posesión.

  Estas dos contraseñas constituyen, por tanto, los datos de activación de la clave privada.

- El acceso a la clave privada del Firmante en Otros dispositivos del tipo dispositivo criptográfico centralizado se realiza mediante la utilización de un nombre de usuario, una contraseña de usuario definida por el Firmante y una contraseña del certificado definida por el Firmante.

  Este nombre de usuario y estas dos contraseñas constituyen, por tanto, los datos de activación de la clave privada.

- El acceso a la clave privada del Creador del sello en DCCS centralizado se realiza, únicamente para su utilización para la firma digital automatizada de documentos electrónicos u otros datos expedidos por el Suscriptor, mediante la utilización de una contraseña definida por el Custodio de claves y configurada por éste en el sistema informático que realiza la firma digital automatizada.

  Esta contraseña constituye, por tanto, los datos de activación de la clave privada.

- El acceso a la clave privada del Creador del sello en Otros dispositivos del tipo dispositivo criptográfico centralizado se realiza, únicamente para su utilización para la firma digital automatizada de documentos electrónicos u otros datos expedidos por el Suscriptor, mediante la utilización de una contraseña definida por el Custodio de claves

y unos códigos proporcionados a éste por SIGNE y configurados por el Custodio de claves en el sistema informático que realiza la firma digital automatizada.

Esta contraseña y estos códigos constituyen, por tanto, los datos de activación de la clave privada.

- El acceso a la clave privada del Firmante o Creador del sello en Otros dispositivos de los tipos dispositivo externo o software se realiza por medio de los datos específicos determinados por el tipo de dispositivo criptográfico donde se haya generado o instalado la clave privada, conforme al nivel de seguridad que el Firmante o Creador del Sello considere adecuado.

  Estos datos específicos determinados por el tipo de dispositivo criptográfico constituyen, por tanto, los datos de activación de la clave privada.

6.2.9. Método de desactivación de la clave privada

- La clave privada de la CA Raíz se desactivará después de su uso, por procedimiento.
- La clave privada de la CA Subordinada de SIGNE sólo se desactivará en situaciones extraordinarias.
- La clave privada del Firmante o Creador del sello en DCCF o DCCS portable o en Otros dispositivos del tipo dispositivo criptográfico portable quedará desactivada una vez que se retire el dispositivo criptográfico de creación de firma electrónica o sello electrónico del dispositivo de lectura.
- La clave privada del Firmante o Creador del sello en DCCF o DCCS centralizado o en Otros dispositivos del tipo dispositivo criptográfico centralizado se desactivará después de cada uso.
- La clave privada del Firmante o Creador del sello en Otros dispositivos de los tipos dispositivo externo o software se desactivará del modo específico determinado por el tipo de dispositivo criptográfico donde se haya generado o instalado la clave privada, conforme al nivel de seguridad que el Firmante o Creador del sello considere adecuado.

6.2.10. Método de destrucción de la clave privada

La destrucción de la clave privada de la CA Raíz de Firmaprofesional o la CA Subordinada de SIGNE se realiza, de acuerdo con un procedimiento documentado de destrucción de claves, por personal autorizado según los roles de confianza, y en presencia de testigos[6] y un auditor interno o externo.

Se realizará un borrado seguro de la clave privada de la CA, utilizando las funciones que

[6] Para ambas CA, al menos una persona con un cargo de relevancia en Firmaprofesional. Para la CA Subordinada de SIGNE, al menos una persona con un cargo de relevancia en SIGNE, a no ser que SIGNE decline su participación.

provee el dispositivo criptográfico hardware (HSM), de forma que no resulten afectadas el resto de claves gestionadas por el dispositivo.

Asimismo, se realizará un borrado seguro de todas las copias de seguridad de la clave privada de la CA, las cuales habrán sido identificadas por Firmaprofesional.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

Los certificados emitidos por la CA Subordinada de SIGNE, y por tanto las claves públicas, se conservarán durante al menos 15 años desde su revocación o expiración.

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

El periodo de uso de un certificado estará determinado por el periodo de validez del mismo.

Un certificado no debe ser usado después del periodo de validez del mismo aunque el tercero que confía en el certificado pueda usarlo para verificar datos históricos.

6.4. Datos de activación

6.4.1. Generación e instalación de los datos de activación

- Los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada de SIGNE fueron generados de forma segura durante la ceremonia de claves.

- Los datos de activación de la clave privada del Firmante o Creador del sello en DCCF o DCCS portable o en Otros dispositivos del tipo dispositivo criptográfico portable son generados en el momento de inicialización del dispositivo.

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

- Los datos de activación de la clave privada del Firmante o Creador del sello en DCCF o DCCS centralizado o en Otros dispositivos del tipo dispositivo criptográfico centralizado son generados al mismo tiempo que las claves en el DCCF o DCCS o dispositivo criptográfico centralizado en el instante previo a la emisión del certificado (contraseña definida por el Firmante o por el Custodio de claves), y/o antes y/o después de la emisión del certificado (en dispositivo criptográfico centralizado, nombre de usuario y contraseña de usuario definida por el Firmante, o códigos proporcionados por SIGNE al Custodio de claves) y/o cada vez que se accede a la clave privada en el DCCF

centralizado (contraseña de un solo uso que el Firmante recibe en su teléfono móvil).

- Los datos de activación de la clave privada del Firmante o Creador del sello en Otros dispositivos de los tipos dispositivo externo o software son generados del modo específico determinado por el tipo de dispositivo criptográfico donde se haya generado o instalado la clave privada, conforme al nivel de seguridad que el Firmante o Creador del sello considere adecuado.

6.4.2. Protección de los datos de activación

Sólo el personal autorizado tiene acceso/conocimiento a/de los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada de SIGNE.

Para los certificados de los Suscriptores, una vez se ha hecho entrega del dispositivo y/o de los datos de activación de la clave privada, es responsabilidad del Firmante o del Custodio de claves firmante mantener la confidencialidad de estos datos.

6.5. Controles de seguridad informática

Firmaprofesional y SIGNE emplean sistemas fiables y productos comerciales para ofrecer los servicios de certificación de SIGNE.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Firmaprofesional o 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.
- En su caso, configuración de antivirus.
- Requerimientos de tráfico de red.

La documentación técnica y de configuración de Firmaprofesional y 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 las plataformas de las CA o las RA incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la CA o las RA 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, las CA y las RA, y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la CA y las RA.
- Mecanismos de recuperación de claves y del sistema de las CA y las RA.

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 los centros de datos de Firmaprofesional y SIGNE.

6.6. Controles de seguridad del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las plataformas de las CA y las RA poseen 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

Firmaprofesional y SIGNE desarrollan las actividades precisas para la formación y concienciación de los empleados en materia de seguridad.

Firmaprofesional y SIGNE exigen, 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

Firmaprofesional y SIGNE mantienen un inventario de activos y documentación, y un procedimiento para garantizar el correcto uso y gestión de este material.

Firmaprofesional y SIGNE dispone de procedimientos documentados de gestión de la información donde se clasifica según su nivel de confidencialidad.

Firmaprofesional y SIGNE disponen de procedimientos documentados de gestión de altas y bajas de usuarios y política de acceso.

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

6.6.2.3 Operaciones de gestión

Firmaprofesional y SIGNE disponen 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 Firmaprofesional y SIGNE y de procedimientos de los respectivos CPD se desarrolla en detalle el proceso de gestión de incidencias.

Firmaprofesional dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

Firmaprofesional y SIGNE tienen 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

Los departamentos técnicos de Firmaprofesional y SIGNE mantienen 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

Firmaprofesional y SIGNE disponen de un procedimiento para el seguimiento de incidencias

y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.7 Procedimientos operacionales y responsabilidades

Firmaprofesional y SIGNE definen actividades asignadas a personas con un rol de confianza distinto, para las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.8 Gestión del sistema de acceso

Firmaprofesional y SIGNE realizan 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 las CA y las RA:

- Se dispone de controles basados en firewalls en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- Se dispone de procedimientos documentados de gestión de altas y bajas de usuarios y política de acceso.
- Se 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 será responsable de sus actos, por ejemplo, por retener logs de eventos.

b) Generación del certificado:

- Las instalaciones 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 las CA.

c) Gestión de la revocación:

- Las instalaciones de las plataformas de las CA y las RA 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 por certificado a las aplicaciones por un operador autorizado (Responsable de revocación). 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 certificado 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 de las CA

Firmaprofesional 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.

Firmaprofesional registra toda la información pertinente de los dispositivos 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 periódicos para asegurar el correcto funcionamiento de los dispositivos.

Los dispositivos criptográficos solo son manipulados por personal confiable.

Las claves privadas de firma de las CA almacenadas en el hardware criptográfico se eliminará una vez que se hayan retirado los dispositivos.

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

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

6.7. Controles de seguridad de la red

Firmaprofesional y SIGNE protegen el acceso físico a los dispositivos de gestión de red y disponen de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

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

6.8. Fuente de tiempo

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

7. Perfiles de los certificados, CRL y OCSP

7.1. Perfil de los certificados

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

- ETSI EN 319 412 conocida como “European profiles for Qualified Certificates”
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- RFC 3739 “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”

El perfil común a todos los certificados es el siguiente:

Campo del certificado	Nombre	Descripción
Version	Nº de versión	V3 (versión del estándar X.509)
Serial Number	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 Firmante o Creador del sello o de la CA*
Extensions …	Extensiones	*Extensiones de los certificados*

7.1.1. Número de versión

Los certificados siguen el estándar de certificados X.509 versión 3.

7.1.2. Extensiones de los certificados

Extensión	Crítica	Posibles Valores
X509v3 Subject Alternative Name	-	En el caso de certificados de usuario: rfc822Name: *email del Firmante o Creador del sello* En el caso de certificados de usuario de firma electrónica: directoryName: 1.3.6.1.4.1.13177.0.1: *Nombre de pila del Firmante* 1.3.6.1.4.1.13177.0.2: *Primer apellido del Firmante* 1.3.6.1.4.1.13177.0.3: *Segundo apellido del Firmante (este campo puede estar vacío)*
X509v3 Basic Constraints	Sí	2 valores posibles en función de si se trata de un certificado de CA o de usuario: CA:FALSE CA:TRUE
X509v3 Key Usage	Sí	En el caso de certificados de usuario: Digital Signature Content Commitment
X509v3 Extended Key Usage	-	En el caso de certificados de usuario: 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	-	Access Method: id-ad-ocsp Access Location: *<URI de acceso al servicio OCSP>* Access Method: id-ad-calssuers Access Location: *<URI de acceso al certificado de la CA emisora>*
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 cualificado) id-etsi-qcs-QcSSCD (a añadir cuando la clave privada se guarda en un DCCF o DCCS) 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 en otras lenguas id-etsi-qcs-QcType: indica el tipo de certificado: • id-etsi-qct-esign, es un certificado de firma electrónica • id-etsi-qct-eseal, es un certificado de sello electrónico

Las extensiones aquí presentadas se 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
1.2.840.113549.1.1.11	sha256WithRSAEncryption	OID del algoritmo de firma
1.2.840.113549.1.1.1	rsaEncryption	OID de Clave pública

7.1.4. Formatos de nombres

Los siguientes atributos del DN son comunes a todos los certificados de firma electrónica.

Atributo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Nombre y apellidos del Firmante*
C, Country	País	*Código de dos letras según ISO 3166-1 del país emisor del código identificativo del Firmante*

Serial Number	Número de serie	*Código identificativo del Firmante, codificado según ETSI EN 319 412-1 con uno de los tipos siguientes: IDC (national identity card number, por ejemplo, DNI en España o Perú), PNO (national personal number, por ejemplo, NIE u otro tipo de NIF distinto de DNI en España, Nº Carné de Extranjería en Perú), PAS (passport number, Nº Pasaporte)* *Ejemplo:* IDCES-00000000G
SN, Surname	Apellidos	*Apellidos (o primer apellido) del Firmante*
GN, Given Name	Nombre de pila	*Nombre de pila del Firmante*

7.1.5. Restricciones de los nombres

Respecto a la codificación de los atributos de los DN de los certificados, siguiendo el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"), se emplea la codificación UTF8String en todos los atributos, contengan o no caracteres especiales, excepto en los atributos en los que es obligatorio utilizar la codificación PrintableString (C, Country; Serial Number).

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

Los certificados incluyen el OID de SIGNE correspondiente a la política de certificación de SIGNE y al dispositivo utilizado, conforme a lo especificado en el apartado 1.4.

Además, los certificados cualificados incluyen el OID correspondiente a la política de certificación europea para los certificados cualificados emitidos a personas físicas sin uso de un DCCF (QCP-n) o con uso de un DCCF (QCP-n-qscd), o para los certificados cualificados emitidos a personas jurídicas sin uso de un DCCS (QCP-l) o con uso de un DCCS (QCP-l-qscd).

Además, los certificados de Sello de Administración, órgano o entidad de derecho público incluyen el OID correspondiente de la política de certificación de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas para los certificados de sello electrónico para la actuación administrativa automatizada, nivel alto o medio.

7.1.7. Sintaxis y semántica de los Policy Qualifiers

Se utilizan dos Policy Qualifiers 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 Policies

La extensión Certificate Policies permite identificar las políticas que SIGNE asocia al certificado y dónde se pueden encontrar dichas políticas.

Está compuesta por 3 elementos: el OID de la política y, en el caso de OID de SIGNE, los dos Policy Qualifiers indicados en el apartado 7.1.7.

7.2. Perfil de CRL

El perfil de las CRL se corresponde con el perfil estándar de CRL X.509 de la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Las CRL son firmadas por la CA que ha emitido los certificados.

7.2.1. Número de versión

Las CRL emitidas por la CA siguen el estándar de CRL X.509 versión 2.

7.2.2. CRL y extensiones

7.2.2.1 CRL de la CA Raíz de Firmaprofesional (ARL)

CAMPOS	VALORES
Versión	V2 (versión del estándar X.509)
Número de CRL	*Número incremental*
Algoritmo de firma	sha256WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	*Fecha de emisión de la CRL, tiempo UTC*
Fecha de próxima actualización	*Fecha 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 certificados revocados (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 CA Subordinada de SIGNE

CAMPOS	VALORES
Versión	V2 (versión del estándar X.509)
Número de CRL	*Número incremental*
Algoritmo de firma	sha256WithRSAEncryption
Emisor (Issuer)	Distinguished Name (DN) del emisor
Fecha efectiva de emisión	*Fecha de emisión de la CRL, tiempo UTC*
Fecha de próxima actualización	*Fecha 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 certificados revocados (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 6960 “Online Certificate Status Protocol – OCSP”.

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

8. Auditorías de cumplimiento y otros controles

8.1. Frecuencia de las auditorías

Se realizarán auditorías periódicas, generalmente con carácter anual.

SIGNE se compromete a realizar las auditorías necesarias.

8.2. Cualificación del auditor

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

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

8.3. Relación entre el auditor y la entidad auditada

Las empresas que realizan las auditorías externas nunca presentan conflictos de intereses que puedan desvirtuar su actuación en su relación con SIGNE.

8.4. Aspectos cubiertos por los controles

Las auditorías verifican los siguientes principios:

a) **Publicación de la información.** El PSC 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 prácticas y política.

b) **Integridad de servicio.** El PSC mantiene controles efectivos para asegurar razonablemente que:

   - La información del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves es identificada y autenticada adecuadamente (para las actividades de registro realizadas por las RA).
   - Se mantiene la integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

c) **Controles generales.** El PSC mantiene controles efectivos para asegurar razonablemente que:

- La información de Suscriptores, Solicitantes, y Firmantes o Custodios de claves está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio del PSC 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 del PSC son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos.

Las auditorías externas de cumplimiento de eIDAS, en general, verifican el cumplimiento de los requisitos establecidos en las normas europeas ETSI EN 319 401, ETSI EN 319 411-1 y ETSI EN 319 411-2.

8.4.1. Auditorías en las Autoridades de Registro

Las Autoridades de Registro que tengan acceso al software para la gestión de certificados son auditadas por SIGNE o por un tercero designado por SIGNE previamente a su puesta en marcha efectiva.

Adicionalmente, se realizan auditorías que comprueban el cumplimiento de los requerimientos exigidos por las Políticas de Certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado.

La periodicidad de las auditorías vendrá determinada por el acuerdo entre 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 tomarán las medidas oportunas para su resolución en el menor tiempo posible. Para no-conformidades graves (que afectan a los servicios críticos, a saber, servicios de revocación y servicios de publicación de CRL), Firmaprofesional y SIGNE se comprometen a su resolución en un plazo máximo de tres meses.

En todo caso se formará un comité de resolución formado por personal de las áreas afectadas y otro de seguimiento formado por los responsables de las áreas afectadas y el Responsable de Seguridad de SIGNE.

8.6. Comunicación de resultados

El auditor comunicará los resultados al Responsable de Seguridad y/o al representante de la Dirección de SIGNE.

9. Otros asuntos legales y de actividad

9.1. Tarifas

9.1.1. Tarifas de emisión de certificado o renovación

Los precios de los servicios de certificación serán facilitados a los clientes o posibles clientes por el Departamento Comercial de SIGNE o por la RA.

9.1.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos por los respectivos Suscriptores, y Firmantes o Custodios de claves es gratuito

9.1.3 Tarifas de revocación o acceso a la información del estado

No se establece ninguna tarifa para la revocación de certificados.

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

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

9.1.4. Tarifas de otros servicios

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

9.2. Responsabilidades económicas

SIGNE, en su actividad como Prestador de Servicios de Confianza, 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 la mínima establecida por el artículo 9.3.b) de la Ley 6/2020, en función del número de servicios de confianza cualificados de los previstos en el Reglamento (UE) 910/2014 que SIGNE preste.

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 personales concretamente con lo dispuesto por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDG).

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 persona, entidad u organización que le haya otorgado el carácter de confidencial, a no ser que ello sea requerido por una autoridad administrativa o judicial.

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 el Texto de Divulgación de PKI (PDS).
- La información contenida en los certificados, puesto que para su emisión el Suscriptor y, en su caso, el Firmante o el Custodio de claves otorgan previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de certificados revocados (CRL), así como las restantes informaciones de estado de revocación.
- En su caso, la información contenida en los repositorios de certificados.
- Cualquier otra información cuya publicidad sea impuesta normativamente.

9.3.3. Responsabilidad en la protección de información confidencial

Es responsabilidad de SIGNE, Firmaprofesional y las RA establecer medidas adecuadas para la protección de la información confidencial.

9.4. Protección de la información personal

9.4.1. Política de protección de datos de carácter personal

En cumplimiento de los requisitos establecidos en la normativa aplicable en materia de protección de datos personales, SIGNE realizará el tratamiento estrictamente necesario de dichos datos con el fin de prestar los servicios de certificación contratados.

Para obtener información adicional sobre el tratamiento de datos personales obtenidos con la referida finalidad se podrá consultar el siguiente enlace: https://www.signe.es/certificacion-electronica/politica-privacidad

9.4.1.1 Aspectos cubiertos

El presente documento describe los procedimientos, requisitos y obligaciones en relación con la obtención y gestión de los datos de carácter personal, cumpliendo con lo establecido en la normativa aplicable en materia de protección de datos personales.

9.4.2. Información tratada como privada

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 el apartado 9.3.2.
- 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 Confianza 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 personal
	Teléfono personal
	Domicilio personal
	País emisor del código identificativo personal
	Código identificativo personal (tipo y número)
	Titulaciones académicas (titulación y organismo emisor)
Ámbito profesional	Nombre de la organización
	Código identificativo de la persona jurídica
	Departamento en la organización
	Cargo, título o rol en la organización
	Domicilio profesional
	E-mail profesional
	Teléfono 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 y, en su caso, el Firmante o el Custodio de claves otorgan previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de certificados revocados (CRL), así como las restantes informaciones de estado de revocación.

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

De acuerdo con la normativa aplicable en materia de protección de datos personales, la información tratada por SIGNE a efectos de lo dispuesto en el párrafo primero del apartado 9.4.1 de la presente DPC está protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en las medidas de seguridad aplicables por SIGNE, Firmaprofesional o la RA, según corresponda.

En caso de violación de la seguridad de los datos personales, SIGNE y/o Firmaprofesional la notificarán a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Asimismo, cuando sea probable que la violación de la

seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

9.4.5. Comunicación y consentimiento para usar datos de carácter personal

El consentimiento del usuario para el tratamiento de los datos personales suministrados para la prestación de servicios contratados, será requerida de manera expresa.

La información personal recabada de los usuarios registrados es almacenada en las bases de datos propiedad, según el caso, bien de Firmaprofesional, bien de SIGNE, bien de la RA. En todo caso, estas entidades deberán implementar 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 normativa aplicable en materia de protección de datos personales 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 o incorrectos, sin prejuicio de las demás acciones legales.

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 usuario cuando sea requerida para ello por una autoridad administrativa o judicial .

9.4.7. Otras circunstancias de publicación de información

Aquéllas descritas en el punto 1 del artículo 6 del RGPD o cualquier otra disposición legal que sea de aplicación.

9.5. Derechos de propiedad intelectual

Propiedad de la DPC

- La propiedad intelectual de esta DPC y de las PC asociadas pertenece a SIGNE, salvo las secciones donde explícitamente se atribuya, en su caso, 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.

9.6. Obligaciones

9.6.1. Obligaciones de la CA

SIGNE se obliga según lo dispuesto en este documento, así como lo dispuesto en el Reglamento eIDAS y la Ley 6/2020, principalmente a:

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

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

c) Informar sobre las modificaciones de esta DPC a los Suscriptores, a los Firmantes o a los Custodios de claves, a las RA que estén vinculadas a la CA y al público en general, incluyendo dichas modificaciones en la tabla inicial de historial de versiones.

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

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

f) En caso de cese de actividad, cumplir lo especificado en el apartado 5.8.1.

g) Enviar al organismo de supervisión el informe de evaluación de la conformidad en los términos previstos en el artículo 20.1 del Reglamento eIDAS.

Por lo que a certificados respecta:

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

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

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

d) En su caso, publicar los certificados emitidos en los repositorios certificados, únicamente si se dispone de la autorización del Suscriptor o el Firmante, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

e) 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:

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

b) No almacenar ni copiar los datos de creación de firma electrónica del Firmante o los datos de creación de sello electrónico del Suscriptor, salvo en caso de su gestión en nombre del titular.

c) Proteger, con el debido cuidado, los datos de creación de firma electrónica del Firmante o los datos de creación de sello electrónico del Suscriptor, en caso de su gestión en nombre del titular, mientras estén bajo su custodia, garantizando que se utilicen, con un alto nivel de confianza, bajo el control exclusivo del Firmante o bajo el control del Creador del sello (Suscriptor), así como su continua disponibilidad.

d) Proteger sus claves privadas de forma segura.

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

9.6.2. Obligaciones de las RA

Las Autoridades de Registro también se obligan en los términos definidos en la presente DPC, así como en el Reglamento eIDAS y la Ley 6/2020, principalmente a:

a) Respetar lo dispuesto en esta DPC y en las PC correspondientes a los tipos de certificados que emita.

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

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

En el ciclo de vida de los certificados:

a) Comprobar la identidad de los Suscriptores, de los Solicitantes, y de los Firmantes o de los Custodios de claves de los 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 Solicitante, y el Firmante o el Custodio de claves.

c) Informar al Solicitante, y al Firmante o al Custodio de claves, antes de la emisión de un certificado, de las obligaciones que asume, la forma en la que debe custodiar los datos o dispositivos de creación de firma electrónica o sello electrónico y/o los datos de acceso a los mismos, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación de firma electrónica o sello electrónico, 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 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, y con los Firmantes o con los Custodios de Claves, 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 revocaciones de los mismos.

9.6.3. Obligaciones de los Solicitantes y los Suscriptores

El Solicitante y el Suscriptor de un certificado estarán obligados 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) Respetar lo dispuesto en los documentos contractuales firmados con la CA y la RA.

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

e) Informar a la mayor brevedad posible de la existencia de alguna causa de revocación.

9.6.4. Obligaciones de los Firmantes y los Custodios de claves

El Firmante o el Custodio de claves de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente 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) Custodiar su clave privada y/o los datos de acceso a la misma, y, en su caso, el DCCF o DCCS de manera diligente.

d) Usar el certificado según lo establecido en la presente DPC y en la PC correspondiente.

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

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

g) Informar a la mayor brevedad posible de la existencia de alguna causa de revocación.

h) 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 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, en todo caso:

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 el Reglamento eIDAS y la Ley 6/2020.

9.8. Responsabilidades

9.8.1. Responsabilidades de la Autoridad de Certificación

SIGNE, en su actividad de prestación de servicios de confianza, responderá por el incumplimiento de lo establecido en las Políticas y Prácticas de certificación (el presente documento, las PC y la PDS) y, allí donde sea aplicable, por lo que dispone el Reglamento eIDAS y la Ley 6/2020.

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 el Reglamento eIDAS y la Ley 6/2020.

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

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

9.8.2. Responsabilidades de la Autoridad de Registro

La RA asumirá toda la responsabilidad en el procedimiento de identificación y autenticación de los Suscriptores, de los Solicitantes, y de los Firmantes o de los Custodios de claves. 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 Firmante o del Custodio de claves, la RA será responsable de la custodia de las claves hasta su entrega al Custodio de claves.

9.8.3. Responsabilidades del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves

Es responsabilidad del Suscriptor, del Solicitante, y del Firmante o del Custodio de claves cumplir con las obligaciones estipuladas en el presente documento y en la PC correspondiente, y en los instrumentos jurídicos vinculantes firmados por los mismos.

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, por el Firmante o por el Custodio de claves, o por los terceros que confían en los certificados, o cualquier otro caso de fuerza mayor.

b) En su caso, por el uso indebido o fraudulento de los repositorios de certificados 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 cifrados mediante los certificados.

e) En relación a acciones u omisiones del Solicitante, del Suscriptor, y del Firmante o del Custodio de Claves:

- Falta de veracidad o exactitud de la información suministrada para emitir el certificado.
- Retraso en la comunicación de las causas de revocación del certificado.
- Ausencia de solicitud de revocación del certificado cuando proceda.
- Negligencia en la conservación de sus datos de creación de firma electrónica o sello electrónico y/o los datos de acceso a los mismos, 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 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 Suscriptor, y al Firmante o al Custodio de claves 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 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 digital.

9.9. Indemnizaciones

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.

9.10. Periodo de validez

9.10.1. Plazo

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

9.10.2. Sustitución y derogación de la DPC

La presente DPC, la PDS y las PC serán derogadas en el momento en que una nueva versión del documento sea publicada en la web de SIGNE.
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 la DPC y en los instrumentos jurídicos vinculantes con los participantes cómo realiza 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 notificará a ésta dicha incidencia.

De modo general, los participantes podrán comunicarse con SIGNE a través de los medios indicados en el apartado 1.6.2.

9.12. Cambios en las especificaciones

9.12.1. Procedimiento para los cambios

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

Todos los cambios en esta DPC y en las PC requerirán nuevas versiones de los documentos. Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

Las nuevas versiones aprobadas de esta DPC y de las PC serán enviadas al organismo de supervisión y publicadas en la página web de SIGNE https://www.signe.es/signe-ac/dpc.

Aquellos cambios que puedan afectar sustancialmente a los Suscriptores, y/o a los Firmantes o a los Custodios de claves serán notificados a los interesados.

Las Autoridades de Registro 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 responsable de la administración de esta DPC y de las PC. Los datos de contacto se encuentran en el apartado 1.6.2.

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 cada nueva versión de la DPC conforme a lo indicado en el apartado 1.2.2.

Será responsabilidad de la organización responsable de la administración de esta DPC y de las PC 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 los Juzgados y Tribunales españoles.

9.14. Normativa aplicable

La normativa aplicable al presente documento, así como a las PC, y a las operaciones que derivan de ellas, es fundamentalmente 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 (Reglamento eIDAS)

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP)
- 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, en la medida en que siga siendo aplicable
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LO 3/2018)

9.15. Cumplimiento de la normativa aplicable

SIGNE manifiesta el cumplimiento de la normativa aplicable.

9.16. Estipulaciones diversas

9.16.1. Cláusula de aceptación completa

Todos los Solicitantes, Suscriptores, Firmantes o Custodios de claves, y terceros que confían en los certificados asumen en su totalidad el contenido de la última versión de este documento y de las PC asociadas.

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

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 los Juzgados y Tribunales españoles.

Una compañía de GRUPOsigne

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
comercial@signe.es