Declaración de Prácticas de Certificación

esFIRMA

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	ESFIRMA
Versión:	1.9

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Oficina de seguridad Fecha: 10/06/2019	Responsable de seguridad Fecha: 12/06/2019	Comité de seguridad Fecha: 14/06/2019

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	esFIRMA	29/04/2016
1.1		Subsanaciones	esFIRMA	02/06/2016
1.2 1.3		Revisión ETSI Revisión tipos de certificados	esFIRMA	19/05/2017
1.4		Revisión ETSI Revisión tipos de certificados Acrónimos y Definiciones	esFIRMA	02/06/2017
1.5	1.3.1 1.3.2 1.3.3.1 1.3.3.2 1.4.1.8 3.1.1.8 4.3.1 6.1.5 9.2.1 9.4 9.6.2 9.6.4	Ajustes referencias normativas, cambio de denominación, cambio certificados	esFIRMA	6/11/2017
1.6	6.1.1	Duración TSA	esFIRMA	20/6/2018
1.7		Corrección referente a la firma en la emisión de certificados sofware	esFIRMA	08/08/2018
1.8		Adaptación por cambio normativo (Reglamento (UE) 910/2014 y Reglamento (UE) 2016/679) y revisión sobre los apartados de renovación.	esFIRMA	13/11/2018
1.9	3.1.1.1 3.1.1.2 3.1.1.7 3.1.1.3 3.1.1.4	Acalaración sobre el segundo apellido opcional. OrganizationIdentifier condicionado a CA/Browser Forum Guidelines	esFIRMA	14/06/2019

	3.1.1.7	Ajuste de errores tipográficos las descripciones de los OID CN del certificado EV de sede opcional		

Índice

ACRÓNIMOS

AC (*o también CA*)	*Certificate Authority* Autoridad de Certificación
AR (o también RA)	*Registration Authority* Autoridad de Registro
CPD	Centro de Proceso de Datos
CPS (o también DPC)	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL (o tambien LRC)	*Certificate Revocation List.* Lista de certificados revocados
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DNI	Documento Nacional de Identidad
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
EV (para SSL)	*Extended Validation* Validación extendida, en certificados SSL.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Módulo de seguridad en Hardware
IETF	*Internet Engineering Task Force*
NIF	Número de Identificación Fiscal
NTP	*Network Time Protocol* Protocolo de tiempo en red.
OCSP	*Online Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PDS	*PKI Disclosure Statements* Texto de Divulgación de PKI.
PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
QSCD (o también DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Dispositivo cualificado de creación de firma/sellos
QCP	*Qualified Certificate Policy*

	Política de certificados cualificados
QCP-n	*Qualified Certificate Policy-natural person* Política de certificados cualificados para personas físicas.
QCP-l	*Qualified Certificate Policy-legal person* Política de certificados cualificados para personas jurídicas.
QCP-n-qscd	*Qualified Certificate Policy-natural person-qscd* Política de certificados cualificados para personas físicas en dispositivo cualificado de firma/sello
QCP-l-qscd	*Qualified Certificate Policy-legal person-qscd* Política de certificados cualificados para personas jurídicas con dispositivo cualificado de firma/sello
RFC	*Request for Comments* Documento RFC
RSA	Rivest-Shamir-Adleman. Tipo de algoritmo de cifrado
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT.
TSA	*Time Stamping Authority* Autoridad de Sellado de Tiempo Electrónico
TSU	*Time Stamping Unit* Unidad de Sellado de Tiempo.
UTC	*Coordinated Universal Time* Tiempo universal coordinado
VPN	*Virtual Private Network.* Red privada virtual

DEFINICIONES

Autoridad de Certificación	*Es la entidad responsable de la emisión y gestión de los certificados digitales.*
Autoridad de Registro	*Entidad responsable de la gestión de las solicitudes, identificación y registro de los solicitantes de un certificado. Puede formar parte de la Autoridad de Certificación o ser ajena.*
Certificado	*Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.*
Clave pública	*Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.*
Clave privada	*Valor matemático conocido únicamente por el Sujeto/Firmante y usado para la creación de una firma digital o el descifrado de datos.* *La clave privada de la AC será usada para firma de certificados y firma de CRL's.* *La clave privada del servicio TSA será usada para firma de los sellos de tiempo.*
CPS	*Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.*
CRL	*Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.*
Datos de Activación	*Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada*
DCCF	*Dispositivo Cualificado de creación de firma. Elemento software o hardware, convenientemente certificado, empleado por el Sujeto/Firmante para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Sujeto/Firmante.*
Firma digital	*El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en*

	conjunción con unos algoritmos conocidos, garantizando de esta manera: *a) que los datos no han sido modificados (integridad)* *b) que la persona que firma los datos es quien dice ser (identificación)* *c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)*
OID	*Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.*
Par de claves	*Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.*
PKI	*Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.*
Solicitante	*En el contexto de este documento, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de la entidad.*
Suscriptor	*En el contexto de este documento la persona jurídica propietaria del certificado (a nivel corporativo)*
Sujeto/Firmante	*En el contexto de este documento, la persona física cuya clave pública es certificada por la AC y dispone de, o tiene acceso de forma exclusiva a, una clave privada válida para generar firmas digitales.*
Parte Usuaria	*En el contexto de este documento, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado*

1. Introducción

1.1. Presentación

Este documento declara las prácticas de certificación de firma electrónica de esFIRMA.

Los certificados que se emiten son los siguientes:

- **De Empleado Público**
  - De Empleado Público nivel Medio
  - De Empleado Público nivel Alto
- **De Sello de Órgano**
  - De Sello de Órgano nivel Medio
- **De Empleado Público con Seudónimo**
  - De Empleado Público con seudónimo nivel Medio
  - De Empleado Público con seudónimo nivel Alto
- **De Sede electrónica**
  - De sede electrónica administrativa nivel Medio
- **De Sello electrónico para TSA/TSU**
  - De sello electrónico para TSU en HSM

1.2. Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de esFIRMA".

1.2.1. Identificadores de certificados

Número OID	Políticas de certificados
	De Empleado Público
1.3.6.1.4.1.47281.1.1.1	*De Empleado Público – Nivel Alto en tarjeta*
1.3.6.1.4.1.47281.1.1.4	*De Empleado Público – Nivel Medio en HSM*
	De Sello de Órgano
1.3.6.1.4.1.47281.1.2.2	*De Sello de Órgano – Nivel Medio en software*
1.3.6.1.4.1.47281.1.2.4	*De Sello de Órgano – Nivel Medio en HSM*

	De Empleado Público con Seudónimo
1.3.6.1.4.1.47281.1.3.1	*De EP con Seudónimo – Nivel Alto en Tarjeta*
1.3.6.1.4.1.47281.1.3.4	*De EP con Seudónimo – Nivel Medio en HSM*
	De Sede electrónica
1.3.6.1.4.1.47281.1.4.2	*De Sede-e EV – Nivel Medio*
	De Sello electrónico para TSA/TSU
1.3.6.1.4.1.47281.1.5.2	*De Sello-e para TSA/TSU en HSM*

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos de esFIRMA, prevalecerá lo establecido en esta Declaración de Prácticas.

esFIRMA se ajusta a la versión actual de las CA/Browser Forum Guidelines FOR Issuance and Management of Extended Validation Certificates publicadas en . En caso de incompatibilidad entre este documento y estas Directrices, estas Directrices prevalecen sobre este documento (8.3 EVCG).

1.3. Participantes en los servicios de certificación

1.3.1. Prestador de servicios de certificación

El prestador de servicios de certificación es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Entidad de Certificación, o presta otros servicios relacionados con la firma electrónica.

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (ANTERIOR AULOCE SA), en adelante ESPUBLICO, con domicilio en la Calle Bari 39 (Edif. Binary Building), C.P. 50.197, de Zaragoza, CIF A-50.878.842, inscrita en el Registro Mercantil de Zaragoza al tomo 2.649, Folio 215, hoja Z-28722, y que opera bajo el nombre comercial esFIRMA, nombre comercial el cual se utilizará a lo largo de este documento para designarla, se trata de un prestador de servicios de certificación que actúa de acuerdo con lo dispuesto en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, y las normas técnicas del ETSI aplicables a la expedición y gestión de certificados cualificados,

principalmente ETSI EN 319 411-1 y ETSI EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, esFIRMA ha establecido una jerarquía de entidades de certificación:

1.3.1.1. esFIRMA AC raíz 2

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave público ha sido autofirmado.

Datos de identificación:

CN:	ESFIRMA AC RAIZ 2
Huella digital SHA-256:	c6:09:f9:4f:9c:ce:20:cb:2b:a0:2e:8b:5b:33:55:20:06:c1:5d:17:78:32:26:11:07:0f:a1:4f:ff:9d:c9:16
Válido desde:	2017-11-02T12:52:43Z
Válido hasta:	2042-11-02T12:52:43Z
Longitud de clave RSA:	4.096 bits

1.3.1.2. esFIRMA AC AAPP 2

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por "esFIRMA AC RAIZ 2".

Datos de identificación:

CN:	ESFIRMA AC AAPP 2
Huella digital SHA-256:	2c:18:23:61:9d:80:73:11:6c:8f:14:8b:d3:85:79:de:9c:05:39:16:02:db:ce:b9:65:73:e4:a1:88:e1:32:6e
Válido desde:	2017-11-02T13:12:47Z
Válido hasta:	2030-11-02T13:12:47Z
Longitud de clave RSA:	4.096 bits

1.3.1.3. Plataforma de Administración Electrónica

Se trata de la plataforma de gestión del ciclo de vida del certificado en exclusiva, para su solicitud, aprobación, emisión y revocación.

Para completar la información sobre las funcionalidades de la Plataforma de Administración Electrónica en los servicios de certificación consultar su documentación.

1.3.2. Registradores

En general, el prestador del servicio de certificación actúa como registrador de la identidad de los suscriptores de certificados.

También son registradores de los certificados sujetos a esta Declaración de Prácticas de Certificación, debido a su condición de certificados corporativos, las unidades designadas para esta función por los suscriptores de los certificados, como la Secretaría de la corporación o el departamento de personal de la Administración, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

Las funciones de registro de los suscriptores se realizan por delegación y de acuerdo con las instrucciones del prestador de servicios de certificación, en los términos que define el Reglamento (UE) 910/2014, y bajo la plena responsabilidad del prestador de servicios de certificación frente a terceros.

1.3.3. Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de identificación y firma electrónica.

Serán entidades finales de los servicios de certificación de esFIRMA las siguientes:

1. Suscriptores del servicio de certificación.
2. Firmantes.
3. Partes usuarias.

1.3.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son las administraciones públicas que los adquieren a esFIRMA para su uso en su ámbito corporativo u organizativo, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio – certificados de sello electrónico o autenticación web–, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado, según se dispone en el epígrafe siguiente.

El suscriptor del servicio de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados, en especial en ETSI EN 319 411-2, secciones 5.4.2 y 6.3.4.e)

1.3.3.2. Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva o tienen bajo su exclusivo control, de acuerdo al régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, las claves de firma digital para identificación y firma electrónica avanzada o cualificada; siendo típicamente las personas titulares o miembros de los órganos administrativos, en los certificados de firma electrónica de órgano, o las personas al servicio de las Administraciones Públicas, en los certificados de empleado público.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación fiscal válido en la jurisdicción de expedición del certificado, o bien con el correspondiente seudónimo en los certificados de este tipo.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la identificación, también se emplea el término más genérico de "persona física identificada en el certificado", siempre con pleno respeto al cumplimiento de la legislación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.3.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Entidad de Certificación.

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1. Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, visibles en la web https://www.esfirma.com

1.4.1.1. Certificado de Empleado Público nivel alto en Tarjeta

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.1.1	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd
2.16.724.1.3.5.7.1	Empleado público español de nivel alto

Los certificados de persona física empleado público nivel alto son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Asimismo, los certificados de persona física empleado público nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 10 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados garantizan la identidad del suscriptor y del firmante, y permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" describe el uso de este certificado.

1.4.1.2. Certificado de Empleado Público nivel medio

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.1.4	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n
2.16.724.1.3.5.7.2	Empleado público español de nivel medio

Los certificados de persona física empleado público nivel medio son certificados cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público nivel medio son gestionados de forma centralizada.

Los certificados de persona física empleado público nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 10 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo "User Notice" describe el uso de este certificado.

1.4.1.3. Certificado de Sello de Órgano nivel medio en software

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.2.2	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l
2.16.724.1.3.5.6.2	Empleado público español de nivel medio

Los certificados de sello electrónico de órgano nivel medio son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados de sello electrónico de órgano nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 9 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones.

Estos certificados garantizan la identidad del suscriptor y del organismo público incluidos en el certificado.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo “User Notice” describe el uso de este certificado.

1.4.1.4. Certificado de Sello de Órgano nivel medio en HSM

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.2.4	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l
2.16.724.1.3.5.6.2	Empleado público español de nivel medio

Los certificados de sello electrónico de órgano nivel medio son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada de acuerdo con el artículo 42 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los certificados de sello electrónico de órgano nivel medio son gestionados de forma centralizada.

Los certificados de sello electrónico de órgano nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 9 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones.

Estos certificados garantizan la identidad del suscriptor y del organismo público incluidos en el certificado.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo “User Notice” describe el uso de este certificado.

1.4.1.5. Certificado de Empleado Público con Seudónimo nivel alto en Tarjeta

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.3.1	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.2	De acuerdo con la política QCP-n-qscd
2.16.724.1.3.5.4.1	Empleado público español con seudónimo nivel alto

Los certificados de persona física empleado público con seudónimo nivel alto son certificados cualificados de acuerdo con el artículo 28 y el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público con seudónimo nivel alto, funcionan con dispositivo seguro de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Asimismo, los certificados de persona física empleado público con seudónimo nivel alto se emiten de acuerdo con los niveles de aseguramiento alto de los perfiles de certificados establecidos en el punto 11 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificada y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo “User Notice” describe el uso de este certificado.

1.4.1.6. Certificado de Empleado Público con seudónimo nivel medio, en HSM

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.3.4	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.0	De acuerdo con la política QCP-n
2.16.724.1.3.5.4.2	Empleado público español con seudónimo nivel medio

Los certificados de persona física empleado público con seudónimo nivel medio son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a empleados públicos para identificarlos (por medio de un seudónimo) como personas al servicio de la Administración, organismo o entidad de derecho público, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

Los certificados de persona física empleado público con seudónimo nivel medio son gestionados de forma centralizada.

Los certificados de persona física empleado público con seudónimo nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de

certificados establecidos en el punto 11 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Estos certificados permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

c) Firma de correo electrónico seguro.
d) Otras aplicaciones de firma digital.

esFIRMA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, esFIRMA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo "User Notice" describe el uso de este certificado.

1.4.1.7. Certificado de Autenticación web, nivel medio

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.4.2	En la jerarquía de la EC esFIRMA

0.4.0.194112.1.4	De acuerdo con la política QCP-web
2.16.724.1.3.5.5.2	Sede electrónica administrativa española de nivel medio

Los certificados de autenticación web de nivel medio son certificados cualificados de acuerdo con el artículo 45 y con el Anexo IV del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a direcciones web para identificarlos como sedes electrónicas administrativas de la Administración, organismo o entidad de derecho público, vinculándolas con ésta, cumpliendo los requisitos establecidos en el artículo 38 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para su identificación y garantizar una comunicación segura con los ciudadanos.

Los certificados de autenticación web de nivel medio se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 8 del documento “Perfiles de Certificados electrónicos” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Digital Signature (para la función de autenticación)
    b. Key Encipherment (para la gestión y transporte de claves)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) El campo “User Notice” describe el uso de este certificado.

1.4.1.8. Certificado de Sello electrónico de TSA/TSU

Este certificado dispone de los siguientes OIDs:

1.3.6.1.4.1.47281.1.5.2	En la jerarquía de la EC esFIRMA
0.4.0.194112.1.1	De acuerdo con la política QCP-l

Los certificados de sello electrónico de TSA/TSU son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo HSM.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
    a. Content Commitment
b) El campo “extend key usage” tiene activada la función:
    a. TimeStamping
c) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
d) El campo “User Notice” describe el uso de este certificado.

1.4.2. Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

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.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de esFIRMA https://www.esfirma.com

El uso de los certificados digitales de forma que se incumpla esta DPC y el resto de documentación aplicable, especialmente el contrato firmado con el suscriptor y los textos de divulgación o PDS tiene la consideración de uso indebido a los efectos legales oportunos, y exime a esFIRMA de cualquier responsabilidad por este uso indebido, ya sea del firmante o de tercero alguno.

esFIRMA no tiene autorización de acceso ni obligación legal de supervisar los datos sobre los que se puede aplicar el uso de una clave certificada. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de esFIRMA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

Los certificados se usan de forma exclusiva y únicamente desde la Plataforma de Administración Electrónica o extensiones y complementos de la misma que la empresa ESPUBLICO pone a disposición del suscriptor.

1.5. Administración de la política

1.5.1. Organización que administra el documento

Oficina de Seguridad de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)
50197 - ZARAGOZA
(+34) 976300110

Identificación Registro	Registro Mercantil de Zaragoza
Tomo	2649
Folio	215
Hoja	Z-28722
CIF	A-50.878.842

1.5.2. Organización que aprueba el documento

Comité de Seguridad de ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)

El comité de seguridad de esFIRMA, formado por el Presidente del mismo, el Responsable de Información y servicio y el Responsable de Seguridad de esFirma, tiene la responsabilidad de la aprobación de esta Declaración de Prácticas.

Tanto las funciones como los miembros de dicho Comité se encuentran definidos en la Política de Seguridad de esFirma.

1.5.3. Datos de contacto de la organización

ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA (esFIRMA)
CALLE BARI 39 (Edif. Binary Building)

50197 - ZARAGOZA
(+34) 976300110

1.5.4. Procedimientos de gestión del documento

El sistema documental y de organización de esFIRMA garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

esFIRMA realiza revisiones como mínimo anuales de este documento.

Tal y como se define en la Política de Seguridad de esFIRMA, la Oficina de Seguridad será la entidad responsable del mantenimiento de este documento.

La Oficina de Seguridad se responsabiliza de la redacción, mantenimiento y administración de la DPC, los textos de divulgación (PDS), hojas de entrega y aceptación, y el resto de documentación jurídica (convenios, contratos, etc.) de esFirma.

Siempre que existan cambios de importancia suficiente en la gestión de los certificados definidos en esta DPC, se creará una nueva revisión de este documento, que constarán en el cuadro inicial de "control de versiones" dentro del apartado de "información general".

La actuación de la Oficina de Seguridad se produce a instancia de su responsable en función de las necesidades que se produzcan.

EsFirma puede realizar cambios que no requieran notificación cuando éstos no afecten directamente a los derechos de los firmantes y suscriptores de los certificados o de los suscriptores de los sellos.

Cuando esFirma vaya a introducir cambios que modifiquen los derechos de los firmantes y suscriptores de los certificados y de los suscriptores de sellos deberá notificarlo públicamente con el objeto que presenten sus comentarios a la Oficina de Seguridad

durante 15 días siguientes a la publicación de los futuros cambios.

Para notificar públicamente los cambios producidos se publicará en el apartado de "documentación" en la página web https://www.esfirma.com

Las revisiones de esta DPC serán publicadas en la web de esFirma tras ser aprobadas por el Comité de Seguridad de Esfirma.

2. Publicación de información y depósito de certificados

2.1. Depósito(s) de certificados

esFIRMA dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de esFIRMA, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación.

2.2. Publicación de información del prestador de servicios de certificación

esFIRMA publica las siguientes informaciones, en su Depósito:

- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.

- Los textos de divulgación (PKI Disclosure Statements - PDS), como mínimo en lengua española y en lengua inglesa.

2.3. Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de esta Declaración de Prácticas de Certificación.

2.4. Control de acceso

esFIRMA no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

esFIRMA emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación

3.1. Registro inicial

3.1.1. Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1. Certificado de empleado público, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
Tipo de certificado OID: 2.16.724.1.3.5.7.1.1	CERTIFICADO CUALIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL ALTO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.7.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.7.1.3	NIF entidad subscription
DNI/NIE del responsable	DNI o NIE del responsable

OID: 2.16.724.1.3.5.7.1.4	
Nombre de pila OID: 2.16.724.1.3.5.7.1.6	Nombre de pila del responsable del certificado
Primer apellido OID: 2.16.724.1.3.5.7.1.7	Primer apellido del responsable del certificado
Segundo apellido OID: 2.16.724.1.3.5.7.1.8	Segundo apellido del responsable del certificado. Opcional.
Correo electrónico OID: 2.16.724.1.3.5.7.1.9	Correo electrónico del responsable del certificado. Opcional.

3.1.1.2. Certificado de empleado público, nivel medio, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Surname	Primer y segundo(opcional) apellido, de acuerdo con documento de identidad (DNI/Pasaporte)
Given Name	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte)
Serial Number	DNI/NIE del empleado
Common Name (CN)	Nombre Apellido1 Apellido2 – NIF del empleado
Tipo de certificado OID: 2.16.724.1.3.5.7.2.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.7.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.7.2.3	NIF entidad subscriptora
DNI/NIE del responsable OID: 2.16.724.1.3.5.7.2.4	DNI o NIE del responsable
Número de autenticación personal OID: 2.16.724.1.3.5.7.2.5	NRP o NIP del responsable del suscriptor del certificado
Nombre de pila OID: 2.16.724.1.3.5.7.2.6	Nombre de pila del responsable del certificado
Primer apellido	Primer apellido del responsable del certificado

OID: 2.16.724.1.3.5.7.2.7	
Segundo apellido OID: 2.16.724.1.3.5.7.2.8	Segundo apellido del responsable del certificado. Opcional.
Correo electrónico OID: 2.16.724.1.3.5.7.2.9	Correo electrónico del responsable del certificad. Opcional.

3.1.1.3. Certificado de sello de órgano, nivel medio, en software

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	SELLO ELECTRONICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.
Tipo de certificado OID: 2.16.724.1.3.5.6.2.1	SELLO ELECTRONICO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.6.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.6.2.3	NIF entidad suscriptora
Denominación del sistema OID: 2.16.724.1.3.5.6.2.5	Denominación del sistema
Correo electrónico OID: 2.16.724.1.3.5.6.2.9	Correo electrónico del responsable del sello

3.1.1.4. Certificado de sello de órgano, nivel medio, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	SELLO ELECTRONICO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Serial Number	DNI/NIE de la organización suscriptora
Common Name (CN)	Denominación de sistema o aplicación de proceso automático.
Tipo de certificado OID: 2.16.724.1.3.5.6.2.1	SELLO ELECTRONICO DE NIVEL MEDIO

Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.6.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.6.2.3	NIF entidad suscriptora
Denominación del sistema OID: 2.16.724.1.3.5.6.2.5	Denominación del sistema

3.1.1.5. Certificado de empleado público con seudónimo, nivel alto, en tarjeta

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1
Pseudonym	Seudónimo obligatorio según ETSI EN 319 412-2 para este tipo de certificados
Common Name (CN)	Seudónimo y el Organismo
Tipo de certificado OID: 2.16.724.1.3.5.4.1.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL ALTO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.4.1.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.4.1.3	NIF entidad suscriptora
Seudónimo OID: 2.16.724.1.3.5.4.1.12	Seudónimo usado por el firmante y autorizado por el suscriptor

3.1.1.6. Certificado de empleado público con seudónimo, nivel medio, en HSM

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado
organizationalUnitName (OU)	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1

Pseudonym	Seudónimo obligatorio según ETSI EN 319 412-2 para este tipo de certificados
Common Name (CN)	Seudónimo y el Organismo
Tipo de certificado OID: 2.16.724.1.3.5.4.2.1	CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO DE NIVEL MEDIO
Nombre de la entidad suscriptora OID: 2.16.724.1.3.5.4.2.2	Nombre de la entidad suscriptora
NIF entidad suscriptora OID: 2.16.724.1.3.5.4.2.3	NIF entidad suscriptora
Seudónimo OID: 2.16.724.1.3.5.4.2.12	Seudónimo usado por el firmante y autorizado por el suscriptor

3.1.1.7. Certificado de autenticación web EV, nivel medio

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado (custodio)
localityName	Ciudad
organizationalUnitName	Descripción del tipo de certificado: SEDE ELECTRONICA
organizationalUnitName	El nombre descriptivo de la sede
serialNumber	El NIF de la entidad responsable
businessCategory	Categoría de la organización: Government Entity
jurisdictionOfIncorporationCountry Name	Jurisdicción
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1, opcional y sólo cuando se ajuste a la versión actual de las CA/Browser Forum Guidelines
Common Name (CN)	Nombre de dominio (DNS) donde residirá el certificado. Opcional.

3.1.1.8. Certificado de sello electrónico de TSA/TSU

Country (C)	"ES"
Organization (O)	Denominación (nombre "oficial" de la organización) del suscriptor
organizationalUnitName (OU)	AUTORIDAD DE CERTIFICACIÓN DE ESFIRMA
Serial Number	DNI/NIE de la organización suscriptora
organizationIdentifier	Identificador de la organización según la norma técnica ETSI EN 319 412-1

Common Name (CN)	Denominación de la TSU

3.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.3. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad/empresa/organización, y en ningún caso se emiten certificados anónimos, a excepción hecha de que, por razones de seguridad pública, los sistemas de firma electrónica puedan referirse sólo al número de identificación profesional del empleado público.

3.1.4. Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” será siempre España por ser los certificados emitidos exclusivamente a las Administraciones Públicas españolas.

El certificado muestra la relación entre una persona física y la Administración, organismo o entidad de derecho público con la que está vinculada, con independencia de la nacionalidad de la persona física. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor la corporación, y la persona física vinculada la persona autorizada a su uso.

En los certificados emitidos a suscriptores españoles, el campo “número de serie” debe incluir el NIF del firmante, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

3.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de esFIRMA.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del Número de Identificación Fiscal, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido de la persona física.
- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido del suscriptor.
- Tipo de Certificado (Campo descripción del certificado).

3.1.6. Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

esFIRMA no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

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

3.2. Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre esFIRMA y el suscriptor, momento en el que se verifica la existencia del suscriptor, y de la documentación aportada justificativa de su identidad y del cargo y/o condición en el cual firma, de conformidad con lo indicado en la normativa de derecho administrativo que sea de aplicación.

La identidad de las personas físicas identificadas en los certificados se valida mediante los registros corporativos de la Administración, organismo o entidad de derecho público suscriptora de los certificados. El suscriptor, mediante certificación administrativa expedida por el Secretario del Ayuntamiento, producirá una certificación de los datos necesarios, y la remitirá a esFIRMA, por los medios que ésta habilite, para el registro de la identidad de los firmantes. Cuando el suscriptor no disponga de Secretaría, esta certificación será emitida por el Responsable del servicio de certificación designado.

El responsable del tratamiento de los datos personales de cada Administración, organismo o entidad de derecho público es cada una de ellas, siendo esFIRMA encargado del tratamiento de dichos datos.

Para evitar cualquier conflicto de intereses las Administraciones Públicas suscriptoras son entidades independientes del Prestador de servicios de confianza “esFIRMA” y de la empresa ESPUBLICO[1].

1 Ap 6.2.2.q) de ETSI EN 319 411-1

3.2.1. Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el firmante desde la Plataforma de Administración Electrónica, al firmar la hoja de aceptación, y su uso en dicha plataforma.

3.2.2. Autenticación de la identidad del suscriptor que actúa mediante un representante

Las personas físicas con capacidad de actuar en nombre de una Administración, organismo o entidad de derecho público suscriptora de los certificados, podrán actuar como representantes de las mismas en relación a lo previsto en esta DPC, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la Administración, organismo o entidad de derecho público suscriptora de los certificados, que exige su reconocimiento por esFIRMA, la cual se realizará mediante el siguiente procedimiento:

1. Un certificado de secretaría del acuerdo del pleno en el que se nombra al representante legal, con los siguientes datos:
    a. como representante:
        i. Nombre y apellidos
        ii. Documento: NIF del representante
    b. Los datos de identificación del suscriptor al que representa:
        i. Nombre de la Administración, organismo o entidad de derecho público.
        ii. Información sobre la extensión y vigencia de las facultades de representación del solicitante.
        iii. Documento: NIF de Administración, organismo o entidad de derecho público.
        iv. Documento: Documentos que sirvan para acreditar los extremos citados de manera fehaciente de conformidad con lo indicado en la normativa de derecho administrativo que sea de aplicación, y su inscripción en el correspondiente registro público si así resulta exigible.

c. Los datos relativos a la representación o la capacidad de actuación que ostenta:
    i. La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin).
    ii. El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
        1. TOTAL. Representación o capacidad total.
        2. PARCIAL. Representación o capacidad parcial.

2. Un contrato de prestación de servicios de certificación que firmará esFIRMA (ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA) y el representante legal de la Administración, que incluya:
3. Un Protocolo que firmará cada operador autorizado (incluyendo sus obligaciones).

Una vez firmados los documentos electrónicamente, se activarán las funciones de RA a los usuarios del Ayuntamiento que figuren en el contrato como operadores autorizados para desempeñar esta función.

3.2.3. Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

El procedimiento para solicitar y generar certificados se realiza a través de un procedimiento electrónico en la herramienta la Plataforma de Administración Electrónica a disposición del suscriptor y de los firmantes.

El procedimiento electrónico para emitir un certificado a una persona física seguirá los siguientes pasos y se generarán los siguientes documentos:

1. Solicitud del Empleado del certificado a través de la Plataforma de Administración Electrónica (con su correspondiente registro de entrada y apertura de expediente)
2. Un certificado de secretaría, o del departamento de personal, en el que se certifica que esa persona está vinculada al Ayuntamiento.

3. Petición firmada por el operador autorizado por la entidad (o por el representante legal), que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA(adjuntando copia del certificado y de la solicitud del empleado).

Para emitir un certificado de Sello electrónico se siguen los siguientes pasos, a través de un procedimiento electrónico en el que se generan los siguientes documentos:

1. Petición del representante legal de la entidad que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA

Para emitir un certificado de Sede se siguen los siguientes pasos, a través de un procedimiento electrónico en el que se generan los siguientes documentos:

1. Petición del representante legal de la entidad que se registra de salida y se notifica a ESPUBLICO SERVICIOS PARA LA ADMINISTRACION SA.

3.2.3.1. En los certificados

La información de identificación de las personas físicas identificadas en los certificados se valida comparando la información de la solicitud de la Administración, organismo o entidad de derecho público suscriptora de los certificados, con los registros de la Administración, organismo o entidad de derecho público a la que está vinculado, generados según lo indicado en el punto 3.2 de esta DPC, asegurando la corrección de la información a certificar.

3.2.3.2. Necesidad de presencia personal

Solicitud de certificados

Para la solicitud de los certificados no se requiere la presencia física directa debido a la relación ya acreditada entre la persona física y la Administración, organismo o entidad de derecho público a la que está vinculada, y a que esta solicitud se realiza por un operador autorizado por el suscriptor en el contrato.

Tampoco es necesaria la presencia física directa del firmante para aceptar el certificado puesto que ésta se puede realizar mediante firma electrónica avanzada.
Durante este trámite se confirma la identidad de la persona física identificada en el certificado.

3.2.3.3. Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la Administración, organismo o entidad de derecho público a la que está vinculada viene dada por su constancia en los Registros de Personal de la Administración, organismo o entidad de derecho público a las que está vinculada la persona física.

3.2.4. Información de suscriptor no verificada

esFIRMA no incluye ninguna información de suscriptor no verificada en los certificados.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

esFirma no realiza renovaciones de certificados. esFirma emitirá un certificado nuevo, siguiendo el procedimiento de solicitud registrado en la Plataforma de Administración Electrónica.

3.3.2. Identificación y autenticación de la solicitud de renovación tras revocación previa

esFIRMA no realiza renovaciones de certificados.

3.4. Identificación y autenticación de la solicitud de revocación

esFIRMA auténtica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor o de la persona física identificada en el certificado, firmada electrónicamente.
- El uso de la "frase de comprobación de identidad", o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona física identificada en el certificado, y que le permite revocar de forma automática su certificado.
- La personación física en una oficina de la entidad suscriptora.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de esFIRMA.

3.5. Autenticación de una petición de suspensión

esFIRMA no realiza suspensiones de certificados. Las peticiones de suspensión son tratadas como peticiones de revocación.

4. Requisitos de operación del ciclo de vida de los certificados

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

La Administración, organismo o entidad de derecho público debe firmar un contrato de prestación de servicios de certificación con esFIRMA.

Asimismo, con anterioridad a la emisión y entrega de un certificado, existe una solicitud de certificados en una hoja de solicitud de certificados por medio de la Plataforma de Administración Electrónica.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre de la Administración, organismo o entidad de derecho público.

4.1.2. Procedimiento de alta y responsabilidades

esFIRMA recibe solicitudes de certificados, realizadas por las Administraciones, organismos o entidades de derecho público públicas.

Las solicitudes se instrumentan mediante un documento en formato electrónico, cumplimentado por la Administración, organismo o entidad de derecho público, cuyo destinatario es esFIRMA, el cual incluirá los datos de las personas a las que se expedirán certificados. La solicitud será realizada por el operador autorizado por el suscriptor (responsable de certificación) y que ha sido identificado en el contrato entre este suscriptor y esFIRMA.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

4.2. Procesamiento de la solicitud de certificación

4.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, esFIRMA se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, esFIRMA verifica la información proporcionada, comprobando que se han cumplido correctamente los requisitos descritos en la sección 3.2.

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación, al ser los certificados, cualificados.

4.2.2. Aprobación o rechazo de la solicitud

esFIRMA aprueba la solicitud del certificado y procede a su emisión y entrega, tras la petición que se produce en la Plataforma de Administración Electrónica.

En caso de sospecha que la información no es correcta o que puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, esFIRMA denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, esFIRMA denegará la solicitud definitivamente.

esFIRMA notifica al solicitante la aprobación o denegación de la solicitud.

esFIRMA podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.2.3. Plazo para resolver la solicitud

esFIRMA atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3. Emisión del certificado

4.3.1. Acciones de la CA durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación mediante el envío de un enlace al dispositivo móvil y/o dirección de correo electrónico que se haya designado por el suscriptor en la petición de certificados, según el procedimiento indicado en el apartado 4.4.2.

Durante el proceso, esFIRMA:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el anexo 1 del Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1.
- Indica la fecha y la hora en que se expidió un certificado.

4.3.2. Notificación de la emisión al suscriptor

esFIRMA notifica la emisión del certificado a la Administración, organismo o entidad de derecho público suscriptora del certificado, y a la persona física identificada en el certificado, a través de sus direcciones de correo electrónico, ya incluidas en la información de la Plataforma de Administración Electrónica.

4.4. Entrega y aceptación del certificado

4.4.1. Responsabilidades de la CA

Durante este proceso, esFIRMA debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona física identificada en el certificado, con la colaboración de la Administración, organismo o entidad de derecho público de acuerdo con lo establecido en las secciones 3.2.2, 3.2.3, y 4.3.1.
- Entregar la hoja de entrega y aceptación del certificado a la persona física identificada en él, la cual dispone de los siguientes contenidos mínimos:

  - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades
  - Información acerca del certificado.
  - Reconocimiento, por parte del firmante, de recibir el certificado y la aceptación de los citados elementos.
  - Régimen de obligaciones del firmante.
  - Responsabilidad del firmante.
  - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
  - La fecha del acto de entrega y aceptación.
- Obtener la firma, escrita o electrónica, de la persona identificada en el certificado.

Cuando sea necesario, la Administración, organismo o entidad de derecho público colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conservando los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a esFIRMA, así como los originales cuando esFIRMA precise de acceso a los mismos.

4.4.2. Conducta que constituye aceptación del certificado

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se avisa al firmante para su aceptación mediante el envío de un enlace al dispositivo móvil y/o dirección de correo electrónico que se haya designado por el suscriptor en la petición de certificados o mediante el sistema de mensajería de la Plataforma de Administración Electrónica.

En los certificados emitidos en software, el certificado y las claves son gestionadas en un HSM, disponiendo el firmante de control exclusivo de su uso.

En los certificados emitidos en tarjeta, estas son enviadas al responsable de certificación del suscriptor, y los correspondientes PINes directamente a la dirección postal del firmante.

Además, la aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación, por medio de la Plataforma de Administración Electrónica.

4.4.3. Publicación del certificado

En el caso del certificado de TSA/TSU, esFIRMA lo publica en su página web.

4.4.4. Notificación de la emisión a terceros

esFIRMA no realiza ninguna notificación de la emisión a terceras entidades.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por el suscriptor o firmante

esFIRMA obliga a lo siguiente:

- Facilitar a esFIRMA información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de aceptación.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Cuando el certificado funcione conjuntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.

- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4.
- Comunicar a esFIRMA y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

esFIRMA obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2. Uso por el suscriptor

4.5.2.1. Obligaciones del suscriptor del certificado

esFIRMA obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de aceptación.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a esFIRMA y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de esFIRMA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de esFIRMA, sin permiso previo por escrito.

4.5.2.2. Responsabilidad civil del suscriptor de certificado

esFIRMA obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.

- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3. Uso por el tercero que confía en certificados

4.5.3.1. Obligaciones del tercero que confía en certificados

esFIRMA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo cualificado de creación de firma (DCCF) tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de esFIRMA, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de esFIRMA, sin permiso previo por escrito.

4.5.3.2. Responsabilidad civil del tercero que confía en certificados

esFIRMA informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6. Renovación de certificados

esFIRMA no realiza renovación de certificados. esFirma emitirá un certificado nuevo, siguiendo el procedimiento de solicitud registrado en la Plataforma de Administración Electrónica.

4.7. Renovación de claves y certificados

4.7.1. Causas de renovación de claves y certificados

No aplica.

4.7.2. Procedimiento con nueva identificación

esFIRMA advertirá al suscriptor de la necesidad de proceder a una nueva personación del firmante y firma de la hoja de aceptación, en aquellos casos en los que así sea necesario por transcurso del plazo legal de identificación de 5 años.

Dicha personación e identificación se realizará de conformidad con lo indicado en el apartado 3.2.

La firma de la hoja de aceptación se realizará de conformidad con lo indicado en el apartado 4.4.2.

4.7.3. Notificación de la emisión del certificado renovado

No aplica por no existir renovaciones.

4.7.4. Conducta que constituye aceptación del certificado

No aplica.

4.7.5. Publicación del certificado

No aplica.

4.7.6. Notificación de la emisión a terceros

esFIRMA no realiza notificación alguna de la emisión a terceras entidades.

4.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.9. Revocación y suspensión de certificados

4.9.1. Causas de revocación de certificados

esFIRMA revoca un certificado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Infracción, por esFIRMA, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.
   c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
   d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
   e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre esFIRMA y el suscriptor.
   b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.
   c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

4) Otras circunstancias:

a) La terminación del servicio de certificación de esFIRMA, de acuerdo con lo establecido en la sección 5.8.

b) El uso del certificado que sea dañino y continuado para esFIRMA. En este caso, se considera que un uso es dañino en función de los siguientes criterios:

- La naturaleza y el número de quejas recibidas.
- La identidad de las entidades que presentan las quejas.
- La legislación relevante vigente en cada momento.
- La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.9.2. Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La persona identificada en el certificado, mediante petición dirigida a esFIRMA o al suscriptor.
- El suscriptor del certificado, mediante petición dirigida a esFIRMA.

4.9.3. Procedimientos de solicitud de revocación

La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor o del firmante.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por esFIRMA, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

esFIRMA podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación[2].

El servicio de revocación se encuentra en la Plataforma de Administración Electrónica, en la que el firmante y el suscriptor gestionan sus certificados.

En caso de que el destinatario de una solicitud de revocación por parte de una persona física identificada en el certificado fuera la entidad suscriptora una vez autenticada la solicitud ésta debe remitir una solicitud en este sentido a esFIRMA.

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor y, a la persona física identificada en el certificado, acerca del cambio de estado del certificado revocado.

esFIRMA no reactiva el certificado una vez ha sido revocado.

4.9.4. Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, y no será superior a las 24 horas[3].

4.9.5. Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, dentro del horario ordinario de operación de esFIRMA, y no será superior a los 60 minutos[4].

2 Ap 6.2.4.a) iii) de ETSI EN 319 411-1

3 Ap 6.2.4.a) vi) de ETSI EN 319 411-1

4 Ap 6.2.4.a) vii) de ETSI EN 319 411-1

4.9.6. Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de esFIRMA.

Las Listas de Revocación de Certificados se publican en el Depósito de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- *CA ROOT:*
  - https://crls2.esfirma.com/acraiz/acraiz2.crl
  - https://crls1.esfirma.com/acraiz/acraiz2.crl
- *CA INTERMEDIA:*
  - https://crls1.esfirma.com/acaapp/acaapp2.crl
  - https://crls2.esfirma.com/acaapp/acaapp2.crl

4.9.7. Frecuencia de emisión de listas de revocación de certificados (LRCs)

esFIRMA emite una LRC al menos cada 24 horas y siempre que se produzca una revocación.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

4.9.8. Plazo máximo de publicación de LRCs

Las CRLs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso supera unos pocos minutos.

4.9.9. Disponibilidad de servicios de comprobación en línea de estado de certificados

esFIRMA informa acerca del estado de revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados en línea desde las direcciones:

- http://ocsp.esfirma.com/acaapp2/
- http://ocsp1.esfirma.com/acaapp2/
- http://ocsp2.esfirma.com/acaapp2/

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de esFIRMA, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

esFIRMA suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito[5].

esFIRMA mantiene disponible la información del estado de revocación pasado el período de validez del certificado[6].

4.9.10. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos, de forma prioritaria, mediante acceso al servicio OCSP.

5 Ap 6.3.10 de ETSI EN 319 411-2

6 Ap 6.3.10.b) de ETSI EN 319 411-2

4.9.11. Otras formas de información de revocación de certificados

De forma alternativa, los terceros que confían en certificados podrán verificar el estado de revocación de los certificados consultando las CRLs más reciente emitida por esFIRMA. Éstas se encuentran publicadas en el sitio web de esFIRMA, así como en las direcciones web indicadas en los certificados.

4.9.12. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de esFIRMA es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de esFIRMA, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.13. Causas de suspensión de certificados

esFIRMA no realiza suspensión de certificados.

4.9.14. Solicitud de suspensión

esFIRMA no realiza suspensión de certificados

4.9.15. Procedimientos para la petición de suspensión

esFIRMA no realiza suspensión de certificados.

4.9.16. Período máximo de suspensión

esFIRMA no realiza suspensión de certificados.

4.10. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

esFIRMA puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11. Servicios de comprobación de estado de certificados

4.11.1. Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, en la web https://www.esfirma.com

También se pueden comprobar mediante acceso al servicio OCSP en las direcciones web indicadas en el apartado 4.9.6

4.11.2. Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.12. Depósito y recuperación de claves

4.12.1. Política y prácticas de depósito y recuperación de claves

esFIRMA no presta servicios de depósito y recuperación de claves.

4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

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

5.1. Controles de seguridad física

esFIRMA ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes, generación técnica de los certificados y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados bajo la plena responsabilidad de esFIRMA, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

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.

5.1.1. Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.
- Fiabilidad del 99,995% mensual

esFIRMA dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos

5.1.2. Acceso físico

El CPD donde se ubica la CA de esFIRMA dispone de la calificación TIER IV.

El acceso físico a las dependencias de esFIRMA donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

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

- El acceso a las salas se realiza con lectores de tarjeta de identificación.

- Para el acceso al rac donde se ubican los procesos criptográficos es necesario la autorización previa de esFIRMA a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3. Electricidad y aire acondicionado

Las instalaciones de esFIRMA disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

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

5.1.4. Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

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

5.1.5. Prevención y protección de incendios

Las instalaciones y activos de esFIRMA cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6. Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7. Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, mediante software especializado que realice un mínimo de 3 pasadas de borrado y con patrones de borrado variable.

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8. Copia de respaldo fuera de las instalaciones

esFIRMA utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

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

5.2. Controles de procedimientos

esFIRMA garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de esFIRMA ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1. Funciones fiables

esFIRMA ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con

las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Administrador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de esFIRMA. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.

5.2.2. Número de personas por tarea

esFIRMA garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes. Especialmente en la manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3. Identificación y autenticación para cada función

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

Cada persona solo 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 tarjetas criptográficas y códigos de activación.

5.2.4. Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de la Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

5.2.5. Sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión del servicio de OCSP.
- Componente/módulo de gestión de la Autoridad de Sellado de Tiempo (TSA)

5.3. Controles de personal

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal que realiza tareas calificadas como confiables, lleva al menos un año trabajando en el centro de producción y tiene contratos laborales fijos.

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

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

esFIRMA se asegura de que el personal de registro es confiable para realizar las tareas de registro.

El Administrador de Registro ha realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, esFIRMA retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.
esFIRMA no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto.

5.3.2. Procedimientos de investigación de historial

esFIRMA realiza comprobaciones sobre los antecedentes de los posibles empleados antes de su contratación o de su acceso al puesto de trabajo.

esFIRMA obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales de acuerdo con 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.

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

5.3.3. Requisitos de formación

esFIRMA forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son actualizados y mejorados de forma periódica. La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de esFIRMA. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4. Requisitos y frecuencia de actualización formativa

esFIRMA actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación

5.3.5. Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6. Sanciones para acciones no autorizadas

esFIRMA dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7. Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por esFIRMA. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a esFIRMA.

5.3.8. Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

esFIRMA produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- 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 AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- Las actividades de los cortafuegos y enrutadores[7]
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de

7 Ap 6.4.5.a) de ETSI EN 319 411-1

certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.

- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas que son usados por los firmantes o custodios[8].

5.4.2. Frecuencia de tratamiento de registros de auditoría

esFIRMA revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

esFIRMA mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

8 Ap 6.4.5.a) de ETSI EN 319 411-2

5.4.3. Período de conservación de registros de auditoría

esFIRMA almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

5.4.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación, borrado o eliminación[9] mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.
Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5. Procedimientos de copia de respaldo

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

esFIRMA tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6. Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de

9 Ap 7.10.f) de ETSI EN 319 401

gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de esFIRMA.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5. Archivos de informaciones

esFIRMA, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1. Tipos de registros archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por esFIRMA (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación

- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación[10].
- Todas aquellas elecciones específicas que el firmante o el suscriptor disponga durante el acuerdo de suscripción[11].
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

esFIRMA es responsable del correcto archivo de todo este material.

5.5.2. Período de conservación de registros

esFIRMA archiva los registros especificados anteriormente durante al menos 15 años.

5.5.3. Protección del archivo

esFIRMA protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

esFIRMA asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

10 Ap 6.4.5.h) de ETSI EN 319 411-1

11 Ap 6.4.5.c) iv) de ETSI EN 319 411-1

5.5.4. Procedimientos de copia de respaldo

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

esFIRMA como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, esFIRMA (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5. Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

esFIRMA dispone de un procedimiento donde describe la configuración de tiempos de los equipos utilizados en la emisión de certificados.
La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día[12].

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

esFIRMA dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

12 Ap 7.10.d) de la ETSI EN 319 401

5.5.7. Procedimientos de obtención y verificación de información de archivo

esFIRMA dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible.

5.6. Renovación de claves

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimientos de gestión de incidencias y compromisos

Son almacenadas copias de seguridad de la siguiente información en instalaciones de almacenamiento externo a esFIRMA, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de esFIRMA son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de esFIRMA.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de esFIRMA, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación, desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Certificación.

En caso de compromiso de la clave privada de esFIRMA puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos[13].

esFIRMA ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario en un centro de datos alternativo.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratará los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

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 AC para implementar dichos procesos.

5.7.4. Continuidad del negocio después de un desastre

esFIRMA restablecerá los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el Plan de continuidad de negocio existente.

13 Ap 6.4.8.g) ii) de ETSI EN 319 411-1

esFIRMA dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.7.5. Gestión de revocaciones

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de continuidad de negocio de esFIRMA.

5.8. Terminación del servicio

esFIRMA asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, esFIRMA desarrolla un Plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios para continuar la finalización de las actividades de revocación.
- Comunicará al Ministerio de Industria, Energía y Turismo, con una antelación mínima de 2 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién, o si se extinguirá su vigencia.
- Comunicará, también el Ministerio de Industria, Energía y Turismo, la apertura de cualquier proceso concursal que se siga contra esFIRMA así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.

- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios, al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Se revocarán los certificados de las Unidades de Sellado de Tiempo (TSU)
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.

6. Controles de seguridad técnica

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves de la entidad de certificación intermedia “ESFIRMA AC AAPP 2” es creado por la entidad de certificación raíz “ESFIRMA AC RAIZ 2” de acuerdo con los procedimientos de ceremonia de esFIRMA, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor CISA. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por esFIRMA.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones Common Criteria EAL 4+ y FIPS 140-2 Nivel 3.

ROOT	4.096 bits	25 años
INTERMEDIA	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	2 años
- Certificado de TSA	4.096 bits	5 años

Más información en las siguientes ubicaciones de las PDS:

CERTIFICADO	PDS
Empleado Público – ALTO 1.3.6.1.4.1.47281.1.1.1	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/EP2-ALTO-SMARTCARD-EN/
Empleado Público – MEDIO 1.3.6.1.4.1.47281.1.1.4	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/EP2-MEDIO-HSM-EN/
Sello-e AAPP – MEDIO Soft 1.3.6.1.4.1.47281.1.2.2	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-SOFT-EN/
Sello-e AAPP – MEDIO HSM 1.3.6.1.4.1.47281.1.2.4	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/SO2-MEDIO-HSM-EN/
EP Seudónimo – ALTO 1.3.6.1.4.1.47281.1.3.1	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/ES2-ALTO-SMARTCARD-EN/
EP Seudónimo – MEDIO 1.3.6.1.4.1.47281.1.3.4	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/ES2-MEDIO-HSM-EN/
Sede electrónica EV MEDIO 1.3.6.1.4.1.47281.1.4.2	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/SE2-MEDIO-SOFT-EN/
TSA en HSM 1.3.6.1.4.1.47281.1.5.2	ESPAÑOL: https://www.esfirma.com/doc-pki/PDS2/TS2-ES/ INGLÉS: https://www.esfirma.com/doc-pki/PDS2/TS2-EN/

6.1.1.1. Generación del par de claves del firmante

Las claves del firmante pueden ser creadas por él mismo mediante dispositivos hardware o software autorizados por esFIRMA.

esFIRMA puede crear las claves únicamente por medio de un DCCF.

esFIRMA nunca genera claves en software para ser enviadas al firmante.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2. Envío de la clave privada al firmante

En certificados en dispositivo seguro de creación de firma la clave privada se encuentra debidamente protegida en el interior de dicho dispositivo seguro.

En certificados en software la clave privada del firmante se crea en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que la clave privada se encuentra debidamente protegida en el interior del sistema informático del firmante.

6.1.3. Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por esFIRMA.

Cuando las claves se generan en un DCCF, esFIRMA se asegura que la clave pública que se remite al prestador de servicios de certificación proviene de un par de claves generadas por dicho DCCF[14].

14 Ap 6.5.1.b) de ETSI EN 319 411-2

6.1.4. Distribución de la clave pública del prestador de servicios de certificación

Las claves de esFIRMA son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las CA root y subordinadas estarán a disposición de los usuarios en la página Web de esFIRMA.

6.1.5. Tamaños de claves

La longitud de las claves de la Entidad de Certificación raíz es de 4096 bits.
La longitud de las claves de la Entidad de Certificación subordinada es de 4096 bits.
La longitud de las claves de la TSA es de 4096 bits.
Las claves de los certificados de entidad final son de 2048 bits.

6.1.6. Generación de parámetros de clave pública

La clave pública de la CA Root, de la CA subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

6.1.7. Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9. Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital y el no repudio.

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

En relación a los módulos que gestionan claves de esFIRMA y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2. Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de **3 de 5** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3. Depósito de la clave privada

esFIRMA no almacena copias de las claves privadas de los firmantes.

6.2.4. Copia de respaldo de la clave privada

esFIRMA realiza copia de backup de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

6.2.5. Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

El suscriptor podrá almacenar las claves entregadas en software durante el periodo de duración del certificado. Posteriormente deberá destruirlas asegurándose antes de que no tiene ninguna información cifrada con la clave pública.

Solo en caso de certificados de cifrado, el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso esFIRMA también guardará copia de la clave privada asociada al certificado de cifrado.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de esFIRMA.

6.2.7. Método de activación de la clave privada

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de esFIRMA.

6.2.8. Método de desactivación de la clave privada

La clave privada de esFIRMA se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n.

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.9. Método de destrucción de la clave privada

Para la desactivación de la clave privada de esFIRMA se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Por su parte el firmante deberá introducir el PIN para la nueva activación.

6.2.10. Clasificación de módulos criptográficos

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de esFIRMA. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en software se podrán destruir mediante el borrado de las mismas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de esFIRMA.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

esFIRMA archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

6.3.2. Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de esFIRMA son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, esFIRMA genera de forma segura los datos de activación.

6.4.2. Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, son protegidos por los poseedores de

las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una contraseña lo más completa posible. El firmante debe recordar dicha contraseña.

6.5. Controles de seguridad informática

esFIRMA emplea sistemas fiables para ofrecer sus servicios de certificación. esFIRMA ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

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

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

6.5.1. Requisitos técnicos específicos de seguridad informática

Cada servidor de esFIRMA incluye las siguientes funcionalidades:

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

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

En el caso que esFIRMA distribuyese dispositivos cualificados de creación de firma, verificará en todo momento que dichos dispositivos continúan certificados como DCCF[15].

La verificación de la certificación del DCCF se realiza durante todo el período de validez del certificado[16]. Si el DCCF perdiera su certificación como tal, esFIRMA avisará a los usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos tal y como se detalla en el documento interno Procedimientos Generales de esFIRMA (esFIRMA_ProcedimientosGenerales_v1r0.pdf)

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por esFIRMA son fiables.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por esFIRMA de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

15 Ap 6.5.1.a) de ETSI 319 411-2

16 Ap 6.5.1.c) de ETSI EN 319 411-2

6.6.2. Controles de gestión de seguridad

esFIRMA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos, son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

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

6.6.2.1. Clasificación y gestión de información y bienes

esFIRMA mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

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

Los documentos están catalogados en cuatro niveles: PÚBLICO, RESTRINGIDO, USO INTERNO y CONFIDENCIAL.

6.6.2.2. Operaciones de gestión

esFIRMA dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de esFIRMA se desarrolla en detalle el proceso de gestión de incidencias.

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

6.6.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son 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.

Planificación del sistema

El departamento de Sistemas de esFIRMA mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

esFIRMA dispone de un procedimiento para el seguimiento de incidencias y su resolución.

Procedimientos operacionales y responsabilidades

esFIRMA define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4. Gestión del sistema de acceso

esFIRMA realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.

- esFIRMA dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- esFIRMA dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de esFIRMA es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

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

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de esFIRMA.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

esFIRMA se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

esFIRMA registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

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

esFIRMA realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.
La clave privada de firma de esFIRMA almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

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

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

6.7. Controles de seguridad de red

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

La información confidencial que se transfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8. Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de esFIRMA son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. Fuentes de Tiempo

esFIRMA tiene un procedimiento de sincronización de tiempo coordinado vía NTP.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen el estándar X.509 versión 3, RFC 3739 y ETSI 101 862 “Qualified Certificate Profile”.

7.1.1. Número de versión

esFIRMA emite certificados X.509 Versión 3

7.1.2. Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de esFIRMA https://www.esfirma.com

De esta forma se permite mantener unas versiones más estables de la DPC y desligarlos de los frecuentes ajustes en los perfiles.

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5. Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

7.1.6. Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1

7.2. Perfil de la lista de revocación de certificados

7.2.1. Número de versión

Las CRL emitidas por esFIRMA son de la versión 2.

7.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960

8. Auditoría de conformidad

esFIRMA ha comunicado el inicio de su actividad como prestador de servicios de certificación por el Ministerio de Industria y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1. Frecuencia de la auditoría de conformidad

esFIRMA lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3. Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con esFIRMA.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica respecto a esFIRMA:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por esFIRMA y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de la AC, ARs y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si esFIRMA es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente a la alta dirección de esFIRMA que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la AC y regenerar la infraestructura.
- Terminar el servicio de la AC.
- Otras acciones complementarias que resulten necesarias.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan a la alta dirección de esFIRMA en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

esFIRMA puede establecer una tarifa por la emisión de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2. Tarifa de acceso a certificados

esFIRMA no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3. Tarifa de acceso a información de estado de certificado

esFIRMA no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4. Tarifas de otros servicios

Sin estipulación.

9.1.5. Política de reintegro

Sin estipulación.

9.2. Capacidad financiera

esFIRMA dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1. Cobertura de seguro

esFIRMA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, con un mínimo asegurado de 3.000.000 de euros.

9.2.2. Otros activos

Sin estipulación.

9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados

esFIRMA dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, con un mínimo asegurado de 3.000.000 de euros.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por esFIRMA:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2. Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

esFIRMA divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa[17], serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

esFIRMA indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5. Divulgación de información por petición de su titular

esFIRMA incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de datos personales

esFIRMA se obliga a cumplir la normativa sobre protección de datos de carácter personal, con las medidas de seguridad correspondientes según se relaciona en 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.

17 Apartado 7.10.c) de la ETSI EN 319 401

esFIRMA obtiene los datos personales que figuran en los ficheros por captación de los datos por parte del SUSCRIPTOR, que debe haberlos obtenido legalmente de quien corresponda, en las condiciones previstas en la normativa sobre firma electrónica y sobre protección de datos de carácter personal.

esFIRMA tiene la condición de encargado del tratamiento de datos personales y, como tal, trata los datos única y exclusivamente para los fines que figuran en esta Declaración de Prácticas de Certificación de acuerdo con las instrucciones del responsable del tratamiento, que es el SUSCRIPTOR y que se encuentran incluidas en el Anexo "*Anexo 1: Para el tratamiento de datos personales por ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. en calidad de ENCARGADO DEL TRATAMIENTO*", que rige el contrato de prestación del servicio "Gestiona" entre el SUSCRIPTOR y ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A.

esFIRMA ha desarrollado una política de privacidad, de acuerdo con 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 ha documentado en esta Declaración de Prácticas de Certificación, así como en el Anexo "Anexo 1: *Para el tratamiento de datos personales por ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A. en calidad de ENCARGADO DEL TRATAMIENTO"* que rige el contrato de prestación del servicio "Gestiona" entre el SUSCRIPTOR y ESPUBLICO SERVICIOS PARA LA ADMINISTRACIÓN S.A., los aspectos, procedimientos y medidas de seguridad y organizativas en cumplimiento del régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014, y del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas.

esFIRMA no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8, en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la normativa en protección de datos personales se protege de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en este documento, que se encuentran alineadas con las obligaciones previstas en 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.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Únicamente esFIRMA goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por esFIRMA contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2. Propiedad de la Declaración de Prácticas de Certificación

Únicamente esFIRMA goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado, conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1.1

9.5.4. Propiedad de claves

Los pares de claves son propiedad de los firmantes de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. Obligaciones de la Entidad de Certificación "esFIRMA"

esFIRMA garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

esFIRMA presta los servicios de certificación conforme con esta Declaración de Prácticas de Certificación.

Con anterioridad de la emisión y entrega del certificado al suscriptor, esFIRMA informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS[18], cumple el contenido del anexo A de la ETSI EN 319 411-1 v1.1.1 (2016-02), documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

18 "PKI Disclosure Statement", o declaración de divulgación de PKI aplicable.

esFIRMA comunica de forma permanente los cambios[19] que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://www.esfirma.com

esFIRMA vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones Error: no se encontró el origen de la referencia, 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

19 Ap 6.2.3.b) de ETSI EN 319 411-1

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

esFIRMA, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

esFIRMA, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

esFIRMA, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación.

Adicionalmente, esFIRMA garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el anexo 1 del Reglamento (UE) 910/2014.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.

- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.3. Rechazo de otras garantías

esFIRMA rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Limitación de responsabilidades

esFIRMA limita su responsabilidad de acuerdo con lo que dispone el régimen de obligaciones y responsabilidades del Reglamento (UE) 910/2014.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

esFIRMA incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de dominio), u otras informaciones

en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

esFIRMA incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6. Caso fortuito y fuerza mayor

esFIRMA incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7. Ley aplicable

esFIRMA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

esFIRMA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en

las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.

- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9. Cláusula de jurisdicción competente

esFIRMA establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

esFIRMA establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.