

POLÍTICA DE CERTIFICACIÓN

CERTIFICATION POLICY (CP)

CERTIFICADOS CORPORATIVOS DE PERSONA JURIDICA

Versión 6.0

INDICE

1	INTRODUCCIÓN.....	3
1.1	Descripción General.....	3
1.2	Identificación del Documento.....	3
2	ENTIDADES PARTICIPANTES.....	4
2.1	Prestador de Servicios de CERTificación (PSC).....	4
2.2	Autoridad de Registro (RA).....	4
2.3	Punto de verificación Presencial.....	4
2.4	Solicitante.....	4
2.5	Suscriptor.....	5
2.6	Firmante.....	5
2.7	Custodio de Claves.....	5
2.8	Tercero que confía en los certificados.....	5
3	CARACTERISTICAS DE LOS CERTIFICADOS.....	6
3.1	Periodo de validez de los certificados.....	6
3.2	Dispositivos de Creación de Firma.....	6
3.3	Uso particular de los certificados.....	6
3.4	Tarifas.....	7
4	PROCEDIMIENTOS OPERATIVOS.....	8
4.1	Proceso de emisión de certificados.....	8
4.2	Revocación de certificados.....	9
4.3	Renovación de certificados.....	9
5	PERFIL DEL CERTIFICADO.....	10
5.1	Nombre distinguido (DN).....	10
5.2	Extensiones de los certificados.....	11

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los **Certificados Corporativos de Persona Jurídica** son certificados reconocidos de persona jurídica según la Ley 59/2003, 19 de diciembre, de Firma Electrónica que identifican al suscriptor y firmante como una Corporación con personalidad jurídica.

La solicitud y emisión de los Certificados Corporativos de Persona Jurídica se realiza a través de las Autoridades de Registro de Firmaprofesional.

En el presente documento se exponen las condiciones particulares referentes a este tipo de certificado. Esta Política de Certificación (en adelante, la “CP”) está sujeta al cumplimiento de la Declaración de Prácticas de Certificación (en adelante, la “CPS”) de Firmaprofesional, a la que incorpora por referencia.

1.2 IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	CP Corporativos de Persona Jurídica
Versión:	6.0
Descripción:	Política de Certificación para Certificados Corporativos de Persona Jurídica
Fecha de Emisión:	15/04/2014
OID	1.3.6.1.4.1.13177.10.1.5.1 (en DSCF) 1.3.6.1.4.1.13177.10.1.5.2 (en otros dispositivos)
Localización	http://www.firmaprofesional.com/cps

Anteriormente, estas Políticas de Certificación recibían los nombres de:

- Tipo II.A - CERTIFICADOS CORPORATIVOS RECONOCIDOS DE ENTIDAD O PERSONA JURÍDICA CON DSCF (1.3.6.1.4.1.13177.10.1.5.1.)
- Tipo II.B - CERTIFICADOS CORPORATIVOS RECONOCIDOS DE ENTIDAD O PERSONA JURÍDICA (1.3.6.1.4.1.13177.10.1.5.2)
- CERTIFICADOS DE PERSONA JURÍDICA EN DSCF (1.3.6.1.4.1.13177.10.1.5.1.)
- CERTIFICADOS DE PERSONA JURÍDICA EN SOFTWARE (1.3.6.1.4.1.13177.10.1.5.2)

2 ENTIDADES PARTICIPANTES

2.1 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (PSC)

Estos certificados deben ser emitidos por Firmaprofesional como Prestador de Servicios de Certificación que emite certificados reconocidos según la Ley 59/2003 de Firma Electrónica.

2.2 AUTORIDAD DE REGISTRO (RA)

La gestión de las solicitudes y emisiones de los certificados será realizada por las entidades que actúen como Autoridades de Registro de Firmaprofesional.

Cada entidad que actúe como RA de Firmaprofesional establecerá:

- Los criterios que se deben cumplir para solicitar un certificado, sin entrar en contradicción con lo estipulado en la CPS y la presente CP.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del firmante, cumpliendo con lo estipulado en la CPS y la presente CP.
- Los dispositivos de creación de firma a utilizar, de entre los que previamente Firmaprofesional haya homologado.

2.3 PUNTO DE VERIFICACION PRESENCIAL

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del suscriptor y en la solicitud y entrega de certificados, la RA podrá delegar estas funciones a una entidad de confianza. Dicha entidad deberá tener una especial vinculación con la RA y una relación de proximidad con los suscriptores de los certificados que justifique la delegación.

Por ejemplo, un Gremio podría actuar como entidad de confianza de una Patronal que actúe como RA de Firmaprofesional, en la identificación y entrega de los certificados a las empresas pertenecientes a dicho Gremio.

La entidad de confianza deberá firmar un acuerdo de colaboración con la RA en el que se acepte la delegación de estas funciones. Firmaprofesional deberá autorizar de manera expresa y previa el modelo de acuerdo a firmar.

2.4 SOLICITANTE

Podrán solicitar estos certificados de persona jurídica sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.

2.5 SUScriptor

El suscriptor de este tipo de certificados es la persona jurídica que consta en el certificado.

2.6 FIRMANTE

El firmante de este tipo de certificados es la persona jurídica que consta en el certificado.

2.7 CUSTODIO DE CLAVES

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

2.8 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Estos certificados son certificados reconocidos que cumplen los requisitos que establece la Ley de Firma Electrónica.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso, tanto cuantitativas como cualitativas, que se contienen en la CPS y en la presente CP.

3 CARACTERÍSTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

El periodo de validez será el que se indique en el propio certificado, con un máximo de 4 años.

3.2 DISPOSITIVOS DE CREACIÓN DE FIRMA

En los casos en que Firmaprofesional pueda garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Seguro de Creación de Firma (DSCF), en cumplimiento de los requisitos establecidos en el artículo 24 de la Ley 59/2003, de 19 diciembre, de Firma Electrónica, esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión "Certificate Policies" con valor OID "1.3.6.1.4.1.13177.10.1.5.1"
- Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" habilitado

En cualquier otro caso, se indicará en el propio certificado mediante los siguientes campos:

- Extensión "Certificate Policies" con valor OID "1.3.6.1.4.1.13177.10.1.5.2"
- Extensión QcStatement con valor "id-etsi-qcs-QcSSCD" deshabilitado

3.3 USO PARTICULAR DE LOS CERTIFICADOS

3.3.1 Usos apropiados de los certificados

Los certificados emitidos por Firmaprofesional podrán usarse en los términos establecidos por la normativa vigente aplicable a la firma electrónica, con las condiciones adicionales que se establecen en la CPS, y en esta CP.

Estos certificados sólo podrán ser utilizados, de acuerdo con el artículo 7.4 de la ley 59/2003, cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en otros casos como la contratación de bienes o servicios, publicaciones de informaciones, la realización de comunicaciones comerciales electrónicas, etc., que sean propios o concernientes a su giro o tráfico ordinario.

Los certificados emitidos bajo esta CP pueden ser utilizados por el custodio de claves con los siguientes propósitos:

- Garantizar la integridad del documento firmado.
- No repudio de origen.
- Identificación de la persona jurídica ante terceros que confíen en los certificados.
- Realización de transacciones comerciales, económicas y financieras, en medio digital.

3.3.2 Usos no autorizados de los certificados

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta CP y en la CPS.

No se recomienda su uso para el cifrado de documentos.

3.4 TARIFAS

Firmaprofesional cobrará al Suscriptor lo acordado en el contrato de prestación de servicios firmado por las partes.

Firmaprofesional podrá establecer las tarifas que considere oportunas a los suscriptores, así como establecer los medios de pago que considere más adecuado en cada caso. Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar con el Departamento Comercial de Firmaprofesional.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISIÓN DE CERTIFICADOS

Los pasos a seguir para la obtención del certificado son los siguientes:

a) Solicitud

Las solicitudes de estos certificados deberán realizarse directamente a Firmaprofesional dirigiéndose a algún colaborador que actúe como RA de Firmaprofesional.

En los casos en que Firmaprofesional ya haya verificado previamente la identidad de la Persona Jurídica y del solicitante, no será necesario realizar verificaciones adicionales. En concreto:

- Si el solicitante dispone de un Certificado Corporativo de Representante Legal vigente emitido por Firmaprofesional.
- Si la Corporación actúa como RA de Firmaprofesional para la emisión de sus propios certificados.

b) Aceptación de la solicitud

Firmaprofesional verificará los datos personales del solicitante y su condición de Representante Legal de la Organización.

Esta verificación se realizará bien mediante una consulta telemática al Registro Mercantil o bien revisando la documentación notarial aportada por el solicitante.

c) Tramitación

Cada Autoridad de Registro de Firmaprofesional tendrá acreditadas a una serie de personas para actuar como **Operador de RA** frente a Firmaprofesional. Los Operadores de RA habrán sido autorizados para realizar esta función y habrán sido previamente instruidos en la operativa de emisión de certificados. Cada Operador de RA dispondrá de un Certificado Digital en DSCF propio, que le permitirá gestionar las solicitudes de certificados de usuarios.

Las fases de la tramitación son las siguientes:

1. Generación de claves

El Operador de RA validará la veracidad y exactitud de los datos del firmante y del solicitante

En caso necesario, el Operador de RA gestionará la generación de claves para el solicitante en un dispositivo de creación firma.

El Operador de RA validará que el solicitante está en posesión de la clave privada (datos de creación de firma) asociada a la clave pública (datos de verificación de firma) incluida en la petición de certificación.

2. Emisión del certificado

El Operador de RA generará la petición de certificado en un formato estándar y la enviará a Firmaprofesional.

Firmaprofesional validará la integridad de la petición y que ha sido generada por un Operador de RA debidamente autorizado. Tras esta validación se procederá a la emisión del certificado.

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

3. Entrega

Una vez se ha generado el certificado, y antes de que la RA pueda entregarlo al solicitante, éste último deberá:

- Personarse ante la RA en cumplimiento del artículo 13 de la Ley 59/2003, salvo en los casos en que esta personación no sea necesaria tal como recoge el propio artículo.
- Aceptar formalmente la entrega del certificado dejando evidencia documental en poder de la RA.

Finalmente, la RA hará entrega del certificado al solicitante, ya sea entregándole el DSCF portable, los mecanismos de autenticación y operación remota de firma electrónica o habilitándole los mecanismos para su descarga y posterior uso.

Mediante estos procedimientos, Firmaprofesional garantiza que ningún firmante dispone del certificado antes de que se haya realizado el proceso de personación requerido en el artículo 13 de la Ley 59/2003.

4.2 REVOCACIÓN DE CERTIFICADOS

Según se especifica en la Declaración de Prácticas de Certificación (CPS)

4.3 RENOVACIÓN DE CERTIFICADOS

Existen dos posibilidades:

- **Emisión de un nuevo certificado:** El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.
- **Proceso de renovación online:** Si la RA dispone del servicio y el suscriptor ha contratado la renovación, éste recibirá una notificación de la RA por correo electrónico para iniciar la renovación a través de la página web de Firmaprofesional.

El período de validez de los certificados renovados online estará condicionado por los requisitos que establece la Ley 59/2003 en su artículo 13.4.

5 PERFIL DEL CERTIFICADO

5.1 NOMBRE DISTINGUIDO (DN)

El DN estos certificados contendrá como mínimo los elementos que se citan con el formato siguiente, siguiendo la "Alternativa 2" propuesta en las especificaciones técnicas relacionadas con la Orden Ministerial HAC/1181/2003 de la Agencia Tributaria (AEAT), de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria. (B.O.E. 15-05-2003).

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	<i>Contendrá el nombre comercial de la empresa</i>
O, Organization	Organización	<i>Contendrá la denominación exacta de la empresa según aparezca en el Registro mercantil</i>
serialNumber	Número de identificación	<i>CIF de la Persona Jurídica</i>
E, E-mail (Opcional)	E-mail	<i>Correo electrónico del solicitante.</i>
ST, State	Ubicación Geográfica	<i>Ámbito geográfico de la entidad.</i>
C, Country	País	<i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i>
1.3.6.1.4.1.18838.1.1 ¹	Número de identificación	<i>NIF del responsable</i>
SN, surName	Apellidos	<i>Apellidos del responsable (como constan en el DNI)</i>
GN, givenName	Nombre de Pila	<i>Nombre propio del responsable (como consta en el DNI)</i>

En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado 7.1.4 de la CPS.

¹OID definido por la Agencia Tributaria (AEAT) destinado a este propósito específico

5.2 EXTENSIONES DE LOS CERTIFICADOS

Extensión	Crítica	Valores
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation Key Encipherment, Data Encipherment, Key Agreement
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Subject Alternative Name (Opcional)	-	<email del suscriptor>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> <URI de la CPS> User Notice : Este es un Certificado Corporativo de Persona Juridica reconocido
QcStatements	-	Id-etsi-qcs-QcCompliance (indicando que el certificado reconocido) Id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DSCF)
X509v3 Issuer Alternative Name (Opcional)	-	URI:http://www.firmaprofesional.com
X509v3 Authority Information Access (Opcional)	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP>