

POLÍTICA DE CERTIFICACIÓN

CERTIFICATION POLICY (CP)

CERTIFICADOS CORPORATIVOS DE COLEGIADO

Versión 5.0

INDICE

1	INTRODUCCIÓN	3
1.1	Descripción general.....	3
1.2	Nombre del Documento de identificación	3
2	ENTIDADES PARTICIPANTES	4
2.1	Autoridades de Certificación (CA)	4
2.2	Autoridad de Registro (RA)	4
2.3	Solicitante	4
2.4	Suscriptor.....	5
2.5	Firmante.....	5
2.6	Custodio de Claves	5
2.7	Tercero que confía en los certificados.....	5
3	CARACTERISTICAS DE LOS CERTIFICADOS	6
3.1	Periodo de validez de los certificados	6
3.2	Tipo de soporte	6
3.2.1	Dispositivo Seguro de Creación de Firma (DSCF).....	6
3.2.2	Soporte en Software	6
3.3	Uso particular de los certificados corporativos de profesional colegiado	7
3.3.1	Limitación en la cuantía de las transacciones.....	7
3.3.2	Firma Delegada	7
3.3.3	Usos apropiados de los certificados.....	7
3.3.4	Usos no autorizados de los certificados	8
3.4	Tarifas.....	8
4	PROCEDIMIENTOS OPERATIVOS.....	9
4.1	Proceso de emisión de certificados	9
4.2	Revocacion de certificados.....	10
4.3	Renovacion de certificados	10
5	PERFIL DE LOS CERTIFICADOS	11
5.1	Nombre distinguido (DN).....	11
5.2	Extensiones de los certificado	12

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los **Certificados Corporativos de Colegiado** son certificados reconocidos de persona física según la Ley 59/2003 de Firma Electrónica que identifican al suscriptor como Colegio Profesional y al firmante como profesional colegiado por dicho Colegio.

Los Certificados Corporativos de Colegiado solo pueden ser utilizados por el propio firmante, actuando como profesional colegiado.

La solicitud y emisión de los Certificados Corporativos de Colegiado se realiza a través de los propios Colegios Profesionales a los que se vincula cada certificado

En el presente documento se exponen las condiciones particulares referentes a este tipo de certificado. Esta Política de Certificación está subordinada al cumplimiento de la Declaración de Prácticas de Certificación (CPS) de Firmaprofesional.

1.2 NOMBRE DEL DOCUMENTO DE IDENTIFICACIÓN

Nombre:	CP Corporativos de Colegiado
Versión:	5.0
Descripción:	Política de Certificación para Certificados Corporativos de Colegiado
Fecha de Emisión:	26/07/2010
OIDs	1.3.6.1.4.1.13177.10.1.1.1 (en DSCF) 1.3.6.1.4.1.13177.10.1.1.2 (en software)
Localización	http://www.firmaprofesional.com/cps

Anteriormente, estas Políticas de Certificación recibían los nombres de:

- Tipo II.A - CERTIFICADOS CORPORATIVOS RECONOCIDOS DE COLEGIADO CON DSCF (1.3.6.1.4.1.13177.10.1.1.1)
- Tipo II.B - CERTIFICADOS CORPORATIVOS RECONOCIDOS DE COLEGIADO (1.3.6.1.4.1.13177.10.1.1.2)
- CERTIFICADOS RECONOCIDOS DE COLEGIADO EN HARDWARE (1.3.6.1.4.1.13177.10.1.1.1)
- CERTIFICADOS RECONOCIDOS DE COLEGIADO EN SOFTWARE (1.3.6.1.4.1.13177.10.1.1.2)

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados Corporativos de Colegiado deben ser emitidos por la CA Subordinada “**AC Firmaprofesional - CA1**”, que emite certificados digitales a Corporaciones Privadas.

2.2 AUTORIDAD DE REGISTRO (RA)

Tal y como viene estipulado en la CPS, la gestión de las solicitudes y emisiones de los certificados será realizada por las entidades que actúen como Autoridades de Registro de Firmaprofesional.

En el caso de los certificados corporativos de colegiado, la función de RA estará desempeñada por los propios Colegios Profesionales. Cada Colegio Profesional será el responsable de la emisión de los certificados a sus propios colegiados.

Cada Colegio Profesional que actúe como RA establecerá:

- Qué criterios 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.
- Los dispositivos de creación de firma a utilizar, que previamente Firmaprofesional haya homologado.

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del solicitante 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 solicitantes de los certificados que justifique la delegación.

Por ejemplo, un Hospital podría actuar como entidad de confianza de un Colegio de Médicos que actúe como RA de Firmaprofesional, en la identificación y entrega de los certificados a los médicos colegiados que trabajen en dicho Hospital.

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

2.3 SOLICITANTE

Podrá solicitar la emisión de un certificado corporativo de colegiado

- Cualquier profesional colegiado en un colegio profesional.
- El propio Colegio Profesional, en nombre del colegiado.

2.4 SUSCRIPTOR

El Colegio Profesional es el Suscriptor de los certificados y por lo tanto el propietario de los certificados emitidos.

2.5 FIRMANTE

El firmante es la persona física identificada por su nombre, apellidos y NIF. El firmante de un Certificado Corporativo de Colegiado debe estar necesariamente colegiado en el Colegio Profesional.

2.6 CUSTODIO DE CLAVES

El custodio de las claves es el propio firmante. El custodio de las claves también puede ser el propio Colegio Profesional siempre que garantice la custodia en un Dispositivo Seguro de Creación de Firma (Hardware Criptográfico Seguro certificado FIPS 140-2, CC EAL 4+ o similar) y que se mantenga el uso de las claves bajo el control exclusivo del firmante.

2.7 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los Certificados Corporativos de Colegiado son certificados reconocidos según la Ley de Firma Electrónica. Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

3 CARACTERÍSTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los Certificados Corporativos de Colegiado tendrán un periodo de validez de 1, 2, 3 o 4 años.

3.2 TIPO DE SOPORTE

Los Certificados Corporativos de Profesional pueden generarse en dos tipos de soporte: Hardware, o Software. Cada Colegio Profesional decidirá el tipo de soporte en el que emite sus certificados.

3.2.1 *Dispositivo Seguro de Creación de Firma (DSCF)*

Las claves privadas de los certificados emitidos en soporte hardware se generan y almacenan en un "Dispositivo Seguro de Creación de Firma (DSCF)", como una Tarjeta Inteligente o un Token criptográfico. Los DSCF proporcionados por Firmaprofesional están certificados de acuerdo con los términos indicados en el artículo 27 de la ley 59/2003

Según la Ley 59/2003 "Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma". Por lo tanto, la utilización de Certificados Corporativos de Colegiado con DSCF permite realizar firmas electrónicas reconocidas cumpliendo con todos los requisitos que marca la ley.

Las claves de certificados generadas en DSCF no pueden ser copiadas de ninguna manera, por lo que si se pierde o se estropea el dispositivo, será necesario realizar un nuevo proceso de emisión de certificado.

Para activar el DSCF será necesario introducir el código de activación (PIN). Si se introduce el PIN tres veces seguidas de manera incorrecta, el dispositivo quedará bloqueado, y por lo tanto inservible. Para desbloquear la tarjeta será necesario introducir el código de desbloqueo (PUK).

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

Los Certificados Corporativos de Colegiado en DSCF están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.1.1) en la extensión "X509v3 Certificate Policies"

3.2.2 *Soporte en Software*

Las claves privadas de los certificados emitidos en soporte software se generan y almacenan en un navegador de Internet, como por ejemplo Microsoft Explorer.

Según la Ley 59/2003 "Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma". Por lo tanto, la utilización de Certificados Corporativos de Colegiado en software no cumple con todos los requisitos que marca la ley para la firma reconocida. Sin embargo de acuerdo con el artículo 21 de la ley 11/2007 los Certificados Corporativos de Colegiado emitidos en software siendo certificados reconocidos, aunque no produzcan firmas reconocidas, serán admitidos por las

Administraciones Públicas siempre y cuando Firmaprofesional ponga a disposición de las Administraciones Públicas la información precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

Los Certificados Corporativos de Colegiado en software pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

Los Certificados Corporativos de Profesional en Software están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.1.2) en la extensión "X509v3 Certificate Policies"

3.3 USO PARTICULAR DE LOS CERTIFICADOS CORPORATIVOS DE PROFESIONAL COLEGIADO

3.3.1 Limitación en la cuantía de las transacciones

La realización de transacciones comerciales, económicas y financieras, en medio digital, realizadas en base a este certificado no podrán exceder el valor máximo definido en la extensión "qcStatements" (OID 1.3.6.1.5.5.7.1.3.) establecido en 60.000€, siempre y cuando esta limitación se indique en el certificado.

3.3.2 Firma Delegada

Los Colegios (como corporaciones de profesionales colegiados) que actúen como RA podrán ofrecer el servicio de Firma Delegada, pudiendo firmar documentos electrónicamente en nombre de sus profesionales colegiados. Para ello deberán obtener una autorización expresa de Firmaprofesional y del propio colegiado, y ambas deberán ser formalizadas contractualmente.

El servicio de Firma Delegada requerirá que el profesional colegiado disponga de un certificado válido, en base a este certificado se generará un certificado duplicado, cuyas claves privadas custodiará la RA en un dispositivo seguro de creación de firma.

La validez de estos certificados duplicados estará subordinada a la validez de los certificados originales de cada colegiado.

3.3.3 Usos apropiados de los certificados

Los certificados emitidos por Firmaprofesional podrán usarse en los términos establecidos por la CPS, y lo establecido en la legislación vigente al respecto.

Los certificados emitidos bajo esta CP pueden ser utilizados con los siguientes propósitos:

- Integridad del documento firmado.
- No repudio de origen.
- Identificación del firmante y su vinculación con el Colegio Profesional.
- Realización de transacciones comerciales, económicas y financieras, en medio digital, siempre que no excedan el valor máximo definido.

Se permite el uso de estos certificados en las relaciones personales del firmante con las Administraciones Públicas y en otros usos estrictamente personales.

3.3.4 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 Política y en la Declaración de Prácticas de Certificación.

No se recomienda su uso para el cifrado de documentos.

3.4 TARIFAS

El precio de los certificados Corporativos de Colegiado dependerá de la duración de los mismos.

Firmaprofesional cobrará al Suscriptor (Colegio Profesional), 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.

Por su parte, cada Colegio Profesional podrá trasladar el coste de los certificados a los colegiados de la manera que estime oportuna en cada caso.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISIÓN DE CERTIFICADOS

El colegio profesional se encargará de tramitar las solicitudes y proceder a la emisión de los certificados tras la firma del contrato de prestación de servicios de certificación con Firmaprofesional.

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

a) Solicitud

El profesional colegiado que desee solicitar un certificado deberá ponerse en contacto con su Colegio Profesional y realizar la solicitud en la forma que cada Colegio Profesional establezca

b) Aceptación de la solicitud

El Colegio Profesional aceptará la solicitud si se cumplen los requisitos establecidos.

c) Tramitación

Una vez aceptada, el Colegio Profesional tramitará la solicitud del certificado, en función del soporte (hardware o software).

d) Generación de claves

El primer paso de la tramitación será la generación de claves según el soporte que se utilice:

- **En software**

El solicitante recibirá por correo electrónico la confirmación de la solicitud, y deberá proceder a la generación de claves en su ordenador siguiendo las instrucciones de la RA.

Una vez el par de claves generadas, el solicitante obtendrá un código que deberá presentar ante la RA para finalizar el proceso de emisión.

- **En hardware**

Se procederá a la activación del dispositivo y seguidamente se entregará a la RA para que genere el par de claves.

e) Emisión del certificado

Una vez las claves generadas, la RA procederá a la emisión del certificado, generando una petición y enviándola a la CA.

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

- Identificarse presencialmente ante la RA, según el procedimiento que ésta le comunique.
- Leer, aceptar y firmar la Hoja de Entrega y Aceptación, que quedará en poder de la RA

f) Entrega

Finalmente, la RA hará entrega del certificado al colegiado.

- **En software:** El colegiado podrá descargarse de forma segura el certificado en su ordenador.
- **En hardware:** La RA entregará el dispositivo al colegiado.

4.2 REVOCACION DE CERTIFICADOS

El colegiado deberá solicitar la revocación de su certificado en caso de pérdida, robo, compromiso de claves u otras causas descritas en la CPS.

Para solicitar la revocación del certificado el colegiado puede:

a) En horario de oficina:

- Ponerse en contacto telefónicamente o presencialmente con su RA.

b) Fuera de horario de oficina

- Revocar online su certificado en la página web de Firmaprofesional.
- Llamar al servicio de revocación 24x7: 902.361.639

Para toda información complementaria referente a la revocación de los certificados, referirse al apartado correspondiente de la CPS.

4.3 RENOVACION DE CERTIFICADOS

Existen dos procedimientos:

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

5 PERFIL DE LOS CERTIFICADOS

5.1 NOMBRE DISTINGUIDO (DN)

El DN de los Certificados Corporativos de Colegiado contendrá como mínimo los elementos que se citan con el formato siguiente. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	<p>Nombre y Apellidos del firmante</p> <p>Adicionalmente se puede incluir el número de colegiado precedido de la palabra "num:" y separado por el carácter "/".</p> <p>Ej: CN = NOMBRE APELL1 APPELL2 / num:4444</p>
E, E-mail	E-mail	Correo electrónico del firmante.
O, Organization	Organización	<p>Nombre del Colegio Oficial que actúa como RA</p> <p>Adicionalmente se puede incluir el código y el número de la RA que gestionó la emisión del certificado, separados por el carácter "/".</p>
OU, Organization Unit	Unidad en la organización	Contendrá el estatus colegial del firmante, En general, "Colegiado".
T, Title	Título	Título o especialidad del firmante
ST, State	Ubicación Geográfica	Ámbito geográfico del firmante
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de identificación	NIF o NIE del firmante
SN, surName	Apellidos	Apellidos del firmante
GN, givenName	Nombre de Pila	Nombre del firmante

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

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

5.2 EXTENSIONES DE LOS CERTIFICADO

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	<email del firmante>
X509v3 Issuer Alternative Name	-	URI:http://www.firmaprofesional.com
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 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	<URI dónde se encuentra el certificado de la CA>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> <URI de la CPS> User Notice : Este es un Certificado Corporativo de Colegiado 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) id-etsi-qcs-QcLimitValue = 60.000