

POLÍTICA DE CERTIFICACIÓN

CERTIFICATION POLICY (CP)

CERTIFICADOS CORPORATIVOS DE PERSONA FISICA

Versión 5.0

INDICE

1	INTRODUCCIÓN	3
1.1	Descripción General.....	3
1.2	Nombre del Documento e 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.....	4
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	Tipos 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.....	7
3.3.1	Limitación en la cuantía de las transacciones.....	7
3.3.2	Usos apropiados de los certificados.....	7
3.3.3	Usos no autorizados de los certificados	7
3.4	Tarifas.....	8
4	PROCEDIMIENTOS OPERATIVOS.....	9
4.1	Proceso de emisión de certificados	9
4.2	Revocacion de certificados.....	11
4.3	Renovacion de certificados	12
5	PERFIL DE LOS CERTIFICADOS	13
5.1	Nombre distinguido (DN).....	13
5.2	Extensiones de los certificados	14

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los **Certificados Corporativos de Persona Física** son certificados reconocidos de persona física según la Ley 59/2003 de Firma Electrónica que identifican al suscriptor como Corporación y al firmante como vinculado a esa Corporación, ya sea como empleado, asociado, colaborador, cliente o proveedor.

Los Certificados Corporativos de Persona Física solo pueden ser utilizados por el propio firmante.

La solicitud y emisión de los Certificados Corporativos de Persona Física se puede realizar a través de las propias organizaciones a las que se vincula cada certificado, actuando como Autoridades de Registro de Firmaprofesional. No obstante también se pueden utilizar otras entidades no vinculadas con el firmante que sean Autoridades de Registro de Firmaprofesional.

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 E IDENTIFICACIÓN

Nombre:	CP Certificados Corporativos de Persona Física
Versión:	5.0
Descripción:	Política de Certificación para Certificados Corporativos de Persona Física
Fecha de Emisión:	26/07/2010
OIDs	1.3.6.1.4.1.13177.10.1.2.1 (en DSCF) 1.3.6.1.4.1.13177.10.1.2.2 (en software)
Localización	http://www.firmaprofesional.com/cps

Anteriormente, estas Políticas de Certificación recibían los nombres de:

- Tipo II.A - CERTIFICADOS RECONOCIDOS DE PERSONA VINCULADA CON DSCF (1.3.6.1.4.1.13177.10.1.2.1)
- Tipo II.B - CERTIFICADOS RECONOCIDOS DE PERSONA VINCULADA (1.3.6.1.4.1.13177.10.1.2.2)
- CERTIFICADOS RECONOCIDOS DE PERSONA VINCULADA EN HARDWARE (1.3.6.1.4.1.13177.10.1.2.1)
- CERTIFICADOS RECONOCIDOS DE PERSONA VINCULADA EN SOFTWARE (1.3.6.1.4.1.13177.10.1.2.2)

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

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

2.2 AUTORIDAD DE REGISTRO (RA)

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

Adicionalmente, la propia Corporación (empresas, entidades privadas o públicas) podrá actuar como Autoridad de Registro de Firmaprofesional para la gestión de las solicitudes y emisiones de los certificados a aquellas personas físicas con las que tenga una vinculación directa, como empleados, colaboradores, clientes. La propia Corporación será el suscriptor de todos estos certificados emitidos.

Cada Corporación 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.

2.3 SOLICITANTE

El solicitante es el representante legal o voluntario (apoderado general) de la Corporación (empresa, entidad privada o pública) que adquiere los certificados para los empleados o personas vinculadas con la indicada Corporación.

Los profesionales autónomos o empresarios individuales, al no disponer de una personalidad jurídica que los represente, podrán solicitar un Certificado Corporativo de Persona Física en el que la identidad de la persona física y de la persona jurídica serán iguales.

2.4 SUSCRIPTOR

La Corporación es el Suscriptor de los certificados y por lo tanto el propietario de los certificados emitidos.

2.5 FIRMANTE

El firmante será la persona física identificada en el certificado por su nombre, apellidos y NIF, que tenga una vinculación (de empleado, colaborador, etc) con el suscriptor.

2.6 CUSTODIO DE CLAVES

El custodio de las claves es el propio firmante. El custodio de las claves también puede ser la propia Corporación 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 Persona Física 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 Persona Física tendrán un periodo de validez de 1, 2, 3 o 4 años

3.2 TIPOS DE SOPORTE

Los Certificados Corporativos de Persona Física pueden generarse en dos tipos de soporte: Hardware, o Software. Cada Corporación 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 de Persona Vinculada 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 usuario y son entregados al suscriptor por la RA en el proceso de emisión del certificado. Tanto el PIN como el PUK pueden ser modificados posteriormente por el usuario utilizando las aplicaciones correspondientes.

Los Certificados Corporativos de Persona Física en DSCF están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.2.1) 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 Persona Física 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 Persona Física 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 Persona Física en software pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

Los Certificados Corporativos de Persona Física en Software están identificados mediante el OID (1.3.6.1.4.1.13177.10.1.2.2) en la extensión "X509v3 Certificate Policies"

3.3 USO PARTICULAR DE LOS CERTIFICADOS

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 están cubiertas por el Seguro de Responsabilidad Civil de Firmaprofesional para transacciones superiores al 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 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 Corporativos de Persona Física deben ser, en general, utilizados dentro del marco de la relación jurídica de servicio entre el empleado y la empresa. En concreto, pueden ser utilizados con los siguientes propósitos:

- Integridad del documento firmado.
- No repudio de origen.
- Identificación del firmante y su vinculación con la entidad que actúa como RA de Firmaprofesional
- Realización de transacciones comerciales, económicas y financieras, en medio digital.

Se permite el uso de estos certificados en las relaciones personales del firmante con las Administraciones Públicas y en otros usos estrictamente personales siempre y cuando no exista una prohibición del suscriptor (empresa, organización, etc)

3.3.3 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 Persona Física dependerá de la duración de los mismos.

Firmaprofesional cobrará al Suscriptor (Corporación), 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

Si la Corporación ya ha firmado el contrato de prestación de servicios de certificación y su representante legal dispone del certificado corporativo de persona física representante, este representante legal estará autorizado a emitir los certificados directamente accediendo a los servicios de Firmaprofesional, tramitando las correspondientes hojas de entrega.

Si la Corporación no tuviera firmado el contrato de prestación de servicios de certificación con Firmaprofesional, deberá ser firmado por el representante legal en el momento de solicitar un certificado corporativo de Persona Física.

En el caso de que el solicitante actúe en representación de otra persona física se deberá obtener la aceptación del certificado por parte del firmante antes de que el certificado pueda ser considerado válido.

En este caso, el certificado se emitirá con un periodo de carencia durante el cual el certificado no será válido. Finalizado el periodo de carencia, si el solicitante dispone de los medios para acceder a la clave privada y no ha conseguido la aceptación formal del certificado por parte del firmante, el solicitante deberá revocar el certificado de inmediato. En caso contrario se le considerará responsable de todos los perjuicios que puedan ocasionarse por el uso del certificado, especialmente los referentes a la protección de datos de carácter personal del firmante.

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

a) Solicitud

Cuando la Corporación se convierte en RA

El solicitante (representante legal de la Corporación o un apoderado de ésta) se encargará de tramitar las solicitudes a Firmaprofesional (o un agente comercial de ésta) por medio de la Hoja de Pedido.

El solicitante podrá solicitar certificados exclusivamente a aquellas personas que tenga identificadas previamente a través de sus procedimientos internos, y que no hayan pasado más de 5 años desde la última identificación, de esta forma se evita que la persona física se deba personar ante Firmaprofesional.

No obstante la persona física en el momento de recoger el certificado deberá firmar la hoja de entrega y aceptación.

Cuando se utiliza un agente comercial como RA

Este agente comercial deberá:

- Identificar a la persona representante legal de la organización externa
- Verificar sus poderes de representación (siguiendo el procedimiento descrito en la Política de Certificación de Certificados de Persona Jurídica de Firmaprofesional)

1. identificar también al resto de vinculados, por lo que es necesario:

- Obtener una autorización firmada del representante legal de la organización con los datos de las personas autorizadas para obtener un certificado de persona vinculada
- Los datos de esta autorización debe incluir: Nombre, DNI y Cargo en la organización de cada persona autorizada
- Cada persona física en el momento de recoger su certificado deberá firmar la hoja de entrega y aceptación.

La petición del certificado deberá ser realizada por el solicitante, cumpliendo con lo descrito en la CPS y con lo siguiente:

- El solicitante deberá estar autorizado a solicitar el certificado por el representante legal de su organización.
- El solicitante deberá entregar la documentación requerida a la RA para tramitar la solicitud.

Empresarios individuales

En caso de tratarse de un empresario individual únicamente se requerirá que el solicitante aporte la documentación necesaria que demuestre que está dado de alta en Seguridad Social como tal, como un recibo bancario con el pago correspondiente.

b) Aceptación de la solicitud

Cuando la Corporación es RA

La aceptación es automática ya que la RA es la misma Corporación, por lo que directamente el representante legal accediendo la base de datos de la Corporación puede comprobar que la persona física pertenece aún a la Corporación

Cuando se utiliza un agente comercial como RA

La RA verificará la identidad del solicitante y la vinculación del suscriptor con la entidad, así como los datos a incluir en el certificado.

c) Tramitación

Una vez aceptada, la RA o la corporación tramitará la solicitud del certificado, en función del soporte que se utilice.

d) Generación de claves

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

- **En software**

El suscriptor 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 suscriptor 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, firmando la petición de generación de certificado y enviándola a la CA.

Una vez el certificado generado, y antes que la RA pueda entregarlo al suscriptor, 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 y el firmante podrá obtener una copia. .

f) Entrega

Finalmente, la RA hará entrega del certificado al suscriptor.

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

4.2 REVOCACION DE CERTIFICADOS

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

Para solicitar la revocación del certificado el suscriptor 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:

- a) **Proceso de renovación presencial:** El suscriptor deberá dirigirse a su RA, y proceder a la generación de un certificado nuevo.
- b) **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.

5 PERFIL DE LOS CERTIFICADOS

5.1 NOMBRE DISTINGUIDO (DN)

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

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	<i>Nombre y Apellidos del firmante</i>
E, E-mail	E-mail	<i>Correo electrónico del firmante</i>
O, Organization	Organización	<i>Nombre del suscriptor (empresa o entidad privada o pública) con la que existe una vinculación con el firmante</i> <i>En caso que el suscriptor sea un autónomo, se puede incluir el nombre comercial de su establecimiento, su CNAE o IAE</i>
1.3.6.1.4.1.4710.1.3.2 ¹	CIF de la Organización	<i>CIF correspondiente a la persona o entidad a la que está vinculado el firmante.</i>
OU, Organization Unit	Unidad en la organización	<i>Contendrá uno de los siguientes valores:</i> <ul style="list-style-type: none"> ▪ <i>El Departamento al que pertenezca el firmante</i> ▪ <i>Tipo de vinculación con la organización.</i>
T, Title	Título	<i>Cargo, título o rol del firmante en la organización.</i>
ST, State	Ubicación Geográfica	<i>Ámbito geográfico de vinculación del firmante.</i>
C, Country	País	<i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i>
serialNumber	Número de Serie	<i>NIF o NIE del firmante.</i>
SN, surName	Apellidos	<i>Apellidos del firmante</i>
GN, givenName	Nombre de Pila	<i>Nombre del firmante</i>

En caso de que el suscriptor 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
- <XXXXXXXX> 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)

¹ OID propiedad de la empresa Safelayer Secure Communications SA, dedicado a contener un Número de Identificación Fiscal (NIF) o un Código de Identificación Fiscal (CIF).

5.2 EXTENSIONES DE LOS CERTIFICADOS

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 reconocido "corporativo de persona física"
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