

# **POLÍTICA DE CERTIFICACIÓN**

## ***CERTIFICATION POLICY (CP)***

# **CERTIFICADOS DE EMPLEADO PÚBLICO**

**Versión 1.0**

## 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 .....	4
2.6	Tercero que confía en los certificados.....	4
3	CARACTERISTICAS DE LOS CERTIFICADOS .....	5
3.1	Periodo de validez de los certificados .....	5
3.2	Tipo de soporte.....	5
3.2.1	Dispositivo Seguro de Creación de Firma (DSCF).....	5
3.2.2	Soporte en Software .....	5
3.3	Uso particular de los certificados .....	6
3.3.1	Usos apropiados de los certificados .....	6
3.3.2	Usos no autorizados de los certificados .....	6
3.4	Tarifas.....	6
4	PROCEDIMIENTOS OPERATIVOS.....	7
4.1	Proceso de emisión de certificados .....	7
4.2	Revocación de certificados .....	9
4.3	Renovación de certificados.....	9
5	PERFIL DE LOS CERTIFICADOS .....	10
5.1	Campos comunes a los dos niveles.....	10
5.1.1	Certificado.....	10
5.1.2	Extensiones de los certificados .....	11
5.2	Nivel ALTO.....	11
5.2.1	Certificado.....	11
5.2.2	Extensiones de los certificados .....	11
5.3	Nivel MEDIO.....	12
5.3.1	Certificado.....	12
5.3.2	Extensiones de los certificados .....	12

# 1 INTRODUCCIÓN

## 1.1 DESCRIPCIÓN GENERAL

Los Certificados Corporativos de Empleado Público son certificados reconocidos que permiten identificar telemáticamente:

- a los suscriptores como Administraciones Públicas
- a los firmantes como personas al servicio de la administración pública, vinculándola con ésta, según los requisitos establecidos en la Ley 11/2007, de 23 de junio, de Accesos Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP).

La finalidad del certificado corporativo de Empleado Público es poder autenticarse frente a los sistemas y ciudadanos y realizar firmas electrónicas reconocidas en los términos establecidos en la Ley 59/2003, de 19 de diciembre de 2003, de Firma Electrónica.

La solicitud y emisión de los certificados corporativos de Empleado Público se realiza a través de las Autoridades de Registro de Firmaprofesional.

Estos certificados pueden emitirse según dos niveles de aseguramiento, dependiendo del soporte en el que se cree y resida el par de claves:

- MEDIO: soporte *software*
- ALTO: dispositivo seguro de creación de firma (DSCF), según lo establecido en la Ley 59/2003, de 19 de diciembre de 2003, de Firma Electrónica.

La presente política sigue las definiciones de los niveles de aseguramiento del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009

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

## 1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

<b>Nombre:</b>	CP Empleado Público
<b>Versión:</b>	1.0
<b>Descripción:</b>	Política de Certificación para Certificados de Empleado Público
<b>Fecha de Emisión:</b>	26/07/2010
<b>OIDs</b>	1.3.6.1.4.1.13177.10.1.22.1 Nivel Alto – DSCF 1.3.6.1.4.1.13177.10.1.22.2 Nivel Medio – <i>Software</i>
<b>Localización</b>	<a href="http://www.firmaprofesional.com/cps">http://www.firmaprofesional.com/cps</a>

## 2 ENTIDADES PARTICIPANTES

### 2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

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

### 2.2 AUTORIDAD DE REGISTRO (RA)

Las Administraciones Públicas podrán actuar como RA para sus funcionarios, empleados y colaboradores, siempre que tenga un contrato de prestación de servicios de certificación de RA con Firmaprofesional.

Firmaprofesional también podrá actuar como RA, cuando así lo establezca un convenio con la Administración Pública que se lo solicite.

### 2.3 SOLICITANTE

Podrá realizar la solicitud del certificado cualquier empleado público de una Administración Pública que sea RA de Firmaprofesional.

### 2.4 SUSCRIPTOR

El suscriptor del certificado será la Administración Pública propietaria del certificado.

### 2.5 FIRMANTE

El firmante será el empleado como persona física, identificada por su nombre, apellidos (de acuerdo con documento de identidad -DNI, pasaporte, ...-) y NIF.

### 2.6 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los Certificados de Empleado Público están reconocidos por **@firma**, la Plataforma de validación y firma electrónica del Ministerio de la Presidencia.

### 3 CARACTERÍSTICAS DE LOS CERTIFICADOS

#### 3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los certificados de Empleado Público tendrán un periodo de validez de 1, 2, 3 o 4 años.

#### 3.2 TIPO DE SOPORTE

##### 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 Empleado Público 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.

##### 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 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 de Empleado Público 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 en software pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

### 3.3 USO PARTICULAR DE LOS CERTIFICADOS

#### 3.3.1 Usos apropiados de los certificados

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

Los certificados corporativos de empleado público deben ser, en general, utilizados dentro del marco de la relación jurídica de servicio entre el empleado público y la Administración. 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.

#### 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 Política y en la Declaración de Prácticas de Certificación.

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)

### 3.4 TARIFAS

El precio de los certificados corporativos de Empleado al Servicio de la Administración Pública, para Autenticación y Firma Electrónica y las condiciones de pago de este tipo de certificados será necesario consultarlas telefónicamente o por mail con Firmaprofesional.

El pago por estos certificados podrá realizarse en efectivo o por transferencia bancaria.

## 4 PROCEDIMIENTOS OPERATIVOS

### 4.1 PROCESO DE EMISIÓN DE CERTIFICADOS

Si la Corporación Pública ya ha firmado el contrato de prestación de servicios de certificación y su representante legal (el Órgano superior unipersonal de representación o el Órgano en quien se delegue o el Responsable de Recursos Humanos) 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 Pública 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.

La corporación o una RA de Firmaprofesional se encargará de tramitar las solicitudes y proceder a la emisión de los certificados cumpliendo siempre con los términos generales descritos en la CPS.

Los pasos a seguir para la obtención del certificado se detallan a continuación:

#### a) Solicitud

Deberá ser realizada por el solicitante, cumpliendo con lo descrito en la CPS y presentando, como mínimo, la documentación siguiente:

- Cuando la tramitación la realiza directamente la Corporación Pública convertida en RA:
  - Una hoja de pedido firmada por el solicitante de la organización con los datos de las personas autorizadas para obtener un certificado corporativo de empleado de la Administración Pública
  - Los datos de esta petición debe incluir: Nombre, DNI y Cargo en la organización de cada persona autorizada
- Cuando la tramitación la realiza una RA que no sea la misma Corporación Pública:
  - Una hoja de pedido firmada por el solicitante y autorizada por el representante legal de la Corporación Pública con los datos de las personas autorizadas para obtener un certificado corporativo de empleado de la Administración Pública
  - Los datos de la petición debe incluir: Nombre, DNI y Cargo en la organización de cada persona autorizada
    - La acreditación por un medio fehaciente de la existencia de la entidad conforme a Derecho
    - La resolución de la Subsecretaria del Ministerio o titular del organismo público competente
    - Opcionalmente, número de identificación del firmante del certificado, que se corresponde con el NRP o NIP.

**b) Aceptación de la solicitud**

- **Cuando la Corporación Pública 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 a Firmaprofesional o 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 solicitud, la Organización pública o la RA tramitará la solicitud del certificado

**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**

La RA procederá a la emisión del certificado, firmando la petición de certificado en formato PKCS#10 y enviándola a la CA.

Una vez que se haya generado el certificado, 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 se quedará en poder de la RA o agente comercial

**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 REVOCACIÓN 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:

1. En horario de oficina:
  - Ponerse en contacto telefónicamente o presencialmente con su RA.
2. 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 RENOVACIÓN 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

Los certificados corporativos de Empleado al Servicio de la Administración Pública, para Autenticación y Firma Electrónica de Firmaprofesional siguen las recomendaciones del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009.

### 5.1 CAMPOS COMUNES A LOS DOS NIVELES

#### 5.1.1 Certificado

El DN de los certificados corporativos de Empleado al Servicio de la Administración Pública, para Autenticación y Firma Electrónica 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
O, Organization	Organización	<i>Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptor del certificado, a la que se encuentra vinculada el empleado.</i>
OU, Organization Unit	Unidad en la organización	<i>"Certificado electrónico de empleado público"</i>
OU, Organization Unit	Unidad en la organización	<i>Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado</i>
OU, Organization Unit	Unidad en la organización	<i>Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP</i>
Title	Puesto o cargo	<i>Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptor del certificado.</i>
SN, Serial Number	NIF	<i>NIF o NIE del empleado público.</i>
Surname	Apellidos (persona física)	<i>Primer y segundo apellidos (de acuerdo con documento de identidad - DNI, pasaporte, ...) + " - DNI " + NIF del empleado público</i>
Given name	Nombre	<i>Nombre de pila, de acuerdo con documento de identidad (DNI, pasaporte, ...)</i>
CN, Common Name	Nombre, apellidos y NIF	<i>Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI (Ver Surname)</i>
C, Country	País	<i>Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".</i>

## 5.1.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	Email de contacto
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	Email protection TLS Web Client Authentication
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> <URI de la CPS>
Qualified Certificate Statements	Sí	qcCompliance qcEuRetentionPeriod: 15 años

## 5.2 NIVEL ALTO

### 5.2.1 Certificado

Campo	Nombre	Descripción
Signature Algorithm	Algoritmo de firma	RsaWithSHA1, con longitud de claves de 2048 o superior

### 5.2.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	User Notice: " Certificado reconocido de personal, nivel alto. Consulte las condiciones de uso en" + URL de la DPC
Qualified Certificate Statements	Sí	qcSSCD
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.3.1.1 = "certificado electrónico de empleado público" OID: 2.16.724.1.3.5.3.1.2 = <O del DN> OID: 2.16.724.1.3.5.3.1.3 = <CIF de la entidad suscriptora> OID: 2.16.724.1.3.5.3.1.4 = <serialNumber del DN> OID: 2.16.724.1.3.5.3.1.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. (tercera entrada <OU del DN>) OID: 2.16.724.1.3.5.3.1.6 = <Given name> OID: 2.16.724.1.3.5.3.1.7 = <Primer apellido del empleado público>

Extensión	Crítica	Valores
		OID: 2.16.724.1.3.5.3.1.8 = <Segundo apellido del empleado público> OID: 2.16.724.1.3.5.3.1.9 = <correo electrónico del empleado público> OID: 2.16.724.1.3.5.3.1.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>) OID: 2.16.724.1.3.5.3.1.11 = <T del DN>

## 5.3 NIVEL MEDIO

### 5.3.1 Certificado

Campo	Nombre	Descripción
Signature Algorithm	Algoritmo de firma	RsaWithSHA1, con longitud de claves de 1024 o superior

### 5.3.2 Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	User Notice: " Certificado reconocido de personal, nivel medio. Consulte las condiciones de uso en" + URL de la DPC
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.3.2.1 = "certificado electrónico de empleado público" OID: 2.16.724.1.3.5.3.2.2 = <O del DN> OID: 2.16.724.1.3.5.3.2.3 = <CIF de la entidad suscriptora> OID: 2.16.724.1.3.5.3.2.4 = <serialNumber del DN> OID: 2.16.724.1.3.5.3.2.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. (tercera entrada <OU del DN>) OID: 2.16.724.1.3.5.3.2.6 = <Given name> OID: 2.16.724.1.3.5.3.2.7 = <Primer apellido del empleado público> OID: 2.16.724.1.3.5.3.2.8 = <Segundo apellido del empleado público> OID: 2.16.724.1.3.5.3.2.9 = <correo electrónico del empleado público> OID: 2.16.724.1.3.5.3.2.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>) OID: 2.16.724.1.3.5.3.2.11 = <T del DN>