

# **POLÍTICA DE CERTIFICACIÓN**

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

### **CERTIFICADOS DE FIRMA DE CODIGO**

**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	Autoridad 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
3.3	Uso particular de los certificados de Firma de Código.....	5
3.3.1	Usos apropiados de los certificados.....	5
3.3.2	Usos no autorizados de los certificados .....	5
3.4	Tarifas.....	5
4	PROCEDIMIENTOS OPERATIVOS.....	6
4.1	Proceso de emisión de certificados.....	6
4.2	Revocación de certificados.....	7
4.3	Renovación de certificados .....	7
5	PERFIL DE LOS CERTIFICADOS .....	8
5.1	Nombre distinguido (DN).....	8
5.2	Extensiones de los certificados .....	8

# 1 INTRODUCCIÓN

## 1.1 DESCRIPCIÓN GENERAL

Los Certificados Genéricos de Firma de Código son certificados emitidos a Corporaciones para la firma de código ejecutable, como por ejemplo applets de JAVA. El Certificado de Firma de Código identifica a una organización como autora y responsable de un determinado código ejecutable.

Los Certificados Genéricos de Firma de Código emitidos por Firmaprofesional no son certificados digitales reconocidos según la Ley 59/2003 de 19 de diciembre de firma electrónica.

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 Firma de Código
<b>Versión:</b>	5.0
<b>Descripción:</b>	Política de Certificación para Certificados de Firma de Código
<b>Fecha de Emisión:</b>	23/07/2010
<b>OIDs</b>	1.3.6.1.4.1.13177.10.1.8.1
<b>Localización</b>	<a href="http://www.firmaprofesional.com/cps">http://www.firmaprofesional.com/cps</a>

Anteriormente, estas Políticas de Certificación recibían los nombres de:

- Tipo II.E - CERTIFICADO PERSONAL DE FIRMA DE CÓDIGO (1.3.6.1.4.1.13177.10.1.7.1)
- Tipo II.E - CERTIFICADO CORPORATIVO DE FIRMA DE CÓDIGO (1.3.6.1.4.1.13177.10.1.8.1)

## 2 ENTIDADES PARTICIPANTES

### 2.1 AUTORIDAD 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)

Firmaprofesional o un intermediario autorizado actuará como Autoridad de Registro en la tramitación de este tipo de certificados.

### 2.3 SOLICITANTE

Podrá realizar la solicitud de un certificado de Firma de Código cualquier persona autorizada por su propia organización para ello.

### 2.4 SUSCRIPTOR

El suscriptor de un certificado de Firma de Código será un la propia Corporación que aparezca en el Certificado.

### 2.5 FIRMANTE

El firmante será el solicitante del certificado y el responsable de custodiar las claves.

### 2.6 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Los certificados de firma de código de Firmaprofesional están reconocidos por Microsoft <http://support.microsoft.com/kb/931125> en todas sus aplicaciones, incluyendo Internet Explorer, y por la Fundación Mozilla <http://hecker.org/mozilla/ca-certificate-list>, incluyendo el navegador Firefox.

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 firma de código tendrán un periodo de validez de 1, 2, 3, 4, 5, 6, 7, 8, 9 o 10 años.

#### 3.2 TIPO DE SOPORTE

Los certificados corporativos de firma de código se emiten en soporte software.

#### 3.3 USO PARTICULAR DE LOS CERTIFICADOS DE FIRMA DE CÓDIGO

##### 3.3.1 Usos apropiados de los certificados

Los certificados corporativos de firma de código únicamente pueden ser utilizados para firmar código ejecutable, como por ejemplo *applets* Java.

El código firmado con un certificado de firma de código garantiza

- La integridad del código firmado.
- La autoría del código firmado

##### 3.3.2 Usos no autorizados de los certificados

No está autorizado cualquier otro uso diferente a la firma de código.

#### 3.4 TARIFAS

El precio de los certificados de firma de código dependerá de la duración de los mismos. El pago por estos certificados podrá realizarse en efectivo o por transferencia bancaria.

Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar telefónicamente o por mail con Firmaprofesional.

## 4 PROCEDIMIENTOS OPERATIVOS

### 4.1 PROCESO DE EMISION 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 Representante Legal, este representante legal estará autorizado a solicitar 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 de firma de código.

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

#### a) Solicitud

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

#### b) Aceptación de la solicitud

##### Cuando la Corporación es RA

La aceptación es automática ya que la RA es la misma Corporación.

##### Cuando se utiliza a Firmaprofesional o un agente comercial como RA

La RA verificará la identidad del solicitante, su vinculación con la entidad, la existencia de ésta, y los datos a incluir en el certificado.

#### c) Tramitación

Una vez aceptada, la RA o la Corporación tramitarán la solicitud del certificado.

#### d) Generación de claves

Las claves de firma serán generadas en los sistemas del solicitante utilizando sus propias aplicaciones compatibles con los estándares de PKI.

El solicitante entregará a la RA una petición de certificado en formato PKCS#10

Generalmente, las herramientas de desarrollo que permiten el uso de firma de código incluyen herramientas para generar claves y peticiones de certificados. Por ejemplo, la JDK de Java incluye las herramientas "keytool" y "jarsigner".

#### 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.
- Recibir la Hoja de Entrega y Aceptación.

#### f) Entrega

Finalmente, la RA hará entrega del certificado 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 firma de código 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	<i>Nombre de la Organización o Nombre del Programador</i>
O, Organization	Organización	<i>Nombre de la Organización</i>

### 5.2 EXTENSIONES DE LOS CERTIFICADOS

Extensión	Crítica	Valores
X509v3 Issuer Alternative Name	-	URI: <a href="http://www.firmaprofesional.com">http://www.firmaprofesional.com</a>
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation
X509v3 Extended Key Usage	-	CodeSigning (1.3.6.1.5.5.7.3.3)
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 de firma de código.