

# CPS IPSCA.v3.0 Rev.00

---

19 de Mayo de 2005

---

**CPS y Políticas de Certificación  
de  
IPS Certification Authority, S.L.**

---

**IPS Certification Authority, S.L. (IPSCA)**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52  
Fax 91 640 20 41  
general@ipsca.com  
<http://www.ipsca.com>



CPS de IPSCA

CPS

Versión 3.0

Fecha de Publicación: Mayo 2005

CPS de IPSCA

2005, IPS Certification Authority, s.l.,

Todos los derechos reservados.

EL PRESENTE DOCUMENTO NO PUEDE SER REPRODUCIDO, DISTRIBUIDO, COMUNICADO PÚBLICAMENTE, ARCHIVADO O INTRODUCIDO EN UN SISTEMA DE RECUPERACIÓN DE INFORMACIÓN, O TRANSMITIDO, EN CUALQUIER FORMA Y POR CUALQUIER MEDIO (ELECTRÓNICO, MECÁNICO, FOTOGRÁFICO, GRABACIÓN O CUALQUIER OTRO), TOTAL O PARCIALMENTE, SIN EL PREVIO CONSENTIMIENTO POR ESCRITO DE IPSCA.

**IPS Certification Authority, S.L. (IPSCA)**  
**CIF B62210695**  
**Edificio ECU**  
**Ctra. De La Coruña, Km. 23,200**  
**28290 – Parque Rozas**  
**(Madrid)**  
**Tel. 91 640 20 52**  
**Fax 91 640 20 41**  
**general@ipsca.com**

---

## Resumen del CPS de IPSCA

---

**IPSCA**

Edificio ECU

Ctra. De La Coruña, Km. 23,200

28290 – Parque Rozas

(Madrid)

Tel. 91 640 20 52

Fax 91 640 20 41

general@ipsca.com

<http://www.ipsca.com>

**IPSCA, Práctica Profesional de Certificación (CPS), resumen:****Garantía**

IPSCA garantiza que ha realizado todos los trámites necesarios para verificar que la información contenida en cualquier certificado emitido por IPSCA es correcta al tiempo de su emisión.

IPSCA también garantiza que cualquier certificado es revocado si en cualquier momento IPSCA cree que los contenidos de un certificado no son correctos o que de cualquier manera la clave asociada a un certificado ha sido comprometida, manipulada o sea objeto de un mal uso. La naturaleza de los trámites que IPSCA realiza para verificar la información contenida en un certificado varía según los tipos de certificación emitidos. En todo caso los trámites efectuados por IPSCA serán suficientes a los efectos de esta garantía. IPSCA no da otras garantías.

**Responsabilidad**

IPSCA acepta la responsabilidad directa e indirecta por cualquier negligencia en el desarrollo de sus prácticas de verificación. IPSCA no se hace responsable de los actos de terceras partes, suscriptores de certificados y de otras entidades ajenas a IPSCA.

**Confidencialidad**

Los contenidos de los certificados emitidos por IPSCA son información pública. IPSCA garantiza que no divulgará cualquier información adicional del suscriptor a ninguna tercera parte bajo ninguna razón, salvo la requerida por los tribunales siempre que éstos tengan jurisdicción para pedir una información específica.

**Fuerza Mayor**

IPSCA no acepta ninguna responsabilidad por cualquier falta de cumplimiento de la garantía, retraso o no cumplimiento del presente Práctica Profesional de Certificación que resulten de eventos fuera de su control como casos de fuerza mayor, guerra, epidemia, terremoto, incendio y cualquier otro evento que sea razonable de catalogar como de fuerza mayor.

**Revocación del Certificado**

IPSCA podrá revocar o suspender certificados de acuerdo con las condiciones establecidas en este CPS y publicará la lista de certificados revocados en una Lista de Certificados Revocados que sea pública y accesible.

### **Mantenimiento de Datos**

IPSCA mantendrá los datos y documentos relativos a la emisión de certificados por un plazo mínimo de 15 años, sin perjuicio del ejercicio del derecho de cancelación sobre los datos de carácter personal.

### **Contenido del Certificado**

Cada certificado emitido por IPSCA tiene por objeto el certificar únicamente la información contenida en el mismo. IPSCA no se hace responsable de ninguna asunción o interpretación relativa a información que no aparezca en el certificado.

### **Obligaciones del Suscriptor**

El suscriptor es el único responsable de la protección de sus claves privadas. Los suscriptores deberán notificar a IPSCA inmediatamente si creen que una clave privada ha sido o puede haber sido objeto de un mal uso de cualquier forma. Los suscriptores podrán ser responsables frente a IPSCA o frente a terceros de cualquier declaración incorrecta que hayan hecho a IPSCA, así como por cualquier consecuencia directa o indirecta derivada de aquéllas declaraciones incorrectas. Tanto los suscriptores como cualquiera que requiera de los servicios de certificación de IPSCA reconocen que han sido advertidos de que deben poseer una formación adecuada en el uso de los mecanismos de clave pública, previamente a pedir un certificado o tomar decisiones sobre la base del mismo.

Los Usuarios garantizan y responden, en cualquier caso, de la veracidad, exactitud, vigencia y autenticidad de los datos facilitados, y se comprometen a mantenerlos debidamente actualizados.

### **Terceras partes**

No se admitirán responsabilidades frente a terceros que se basen en un certificado emitido por IPSCA si aquellos terceros tuviesen indicios o constancia de que el certificado o su clave pública asociada han sido objeto de manipulación o mal uso. Tales indicios incluyen aunque no se limitan a: los contenidos del certificado, la información incorporada al certificado por referencia así como los contenidos de esta PPC y la Lista de Certificados Revocados publicada por IPSCA.

### **Legislación aplicable**

Para asegurar la uniformidad en los procedimientos y en la interpretación para todos los

usuarios, con independencia de su nacionalidad o país de residencia, la interpretación, validez y aplicación de esta CPS serán gobernados bajo la legislación española.

### **Proceso de Resolución de Conflictos**

En el caso de que se produzca cualquier reclamación o conflicto derivado de la emisión de un certificado por parte de IPSCA, el reclamante debe notificar a IPSCA por escrito y por correo certificado de la naturaleza exacta de la reclamación. El reclamante debe dejar un tiempo razonable a IPSCA para permitir resolver la reclamación antes de invocar cualquier proceso de resolución de conflictos.

En el caso de que IPSCA no sea capaz de resolver la reclamación, las partes intentarán acordar un proceso de arbitraje para resolver la disputa mediante arbitraje. El arbitraje deberá ser final y vinculante.

En el caso de que las partes no llegaran a un acuerdo para resolver la situación a través de arbitraje, las partes se someterán, con renuncia expresa o cualquier otro fuero, a los Juzgados y Tribunales de la ciudad de Madrid. Ninguna otra jurisdicción será aplicable para resolver las reclamaciones que pudieran derivarse de certificados emitidos por IPSCA.

---

## **Documento integro**

### **CPS de IPSCA**

---

**IPS Certification Authority, S.L. (IPSCA)**

Edificio ECU

Ctra. de La Coruña, Km. 23,200

28290 - Parque Rozas

(Madrid)

Tel. 91 640 20 52

Fax 91 640 20 41

general@ipsca.com

<http://www.ipsca.com>

## **1 INTRODUCCIÓN**

### **1.1 Presentación**

El presente documento constituye el CPS de IPSCA, donde se definen los mecanismos relacionados con la práctica de certificación de IPSCA. Esta Declaración de Prácticas de Certificación (CPS) de IPSCA cumple con lo dispuesto en [la CPS de Internet Publishing Services S.L. \(IPS\)](#), empresa que ha emitido un Certificado para CA de Segundo Nivel a IPSCA.

El presente CPS presenta las prácticas que IPSCA, sus entidades emisoras (IAs), y las IAs autorizadas ajenas a IPSCA que prestan los servicios de certificación pública (PCS), utilizan para la emisión y gestión de certificados y en el mantenimiento de una infraestructura de clave pública (PKI) basada en certificados. La CPS detalla y controla el proceso de certificación. Los PCS abarcan la emisión, la gestión, la utilización, la suspensión, la revocación y la renovación de certificados. La CPS describe, como establece la legislación aplicable, las obligaciones legales y, proporcionar información a todas las partes que crean, utilizan y validan certificados en el contexto de los PCS. Las partes que actúan en los PCS de IPSCA están ligadas a sus obligaciones en virtud de sus contratos con IPSCA, las IAs de IPSCA y las IAs ajenas a IPSCA que emiten, gestionan, suspenden, revocan y renuevan certificados en los PCS de IPSCA.

### **1.2. Estructura**

El CPS regula el de ciclo de vida del certificado y describe el proceso de certificación. La estructura de este CPS es la siguiente:

## **1 INTRODUCCIÓN**

### **1.1 Presentación.**

### **1.2 Estructura.**

### **1.3 Identificación.**

- 1.3.1 Autoridad de Certificación.
- 1.3.2 Autoridad de Registro.
- 1.3.3 Suscriptor.
- 1.3.4 Solicitante.
- 1.3.5 Usuario.

**1.4 Comunidad de usuarios y aplicabilidad.**

- 1.4.1 Autoridad de Certificación.
- 1.4.2 Autoridad de Registro.
- 1.4.3 Suscriptor.
- 1.4.4 Solicitante.
- 1.4.5 Usuario.

**1.5 Tipos de Certificados.**

- 1.5.1 B1. Certificados de Correo con validez mensual/anual.
- 1.5.2 B3. Certificado Personal Presencial.
- 1.5.3 B3 Colegial
- 1.5.4 A1. Certificados de Servidor.

**1.6 Limitación en el uso de los Certificados.****1.7 Detalles de contacto.****2 ASPECTOS GENERALES.****2.1 Obligaciones.**

- 2.1.1 Obligaciones de IPSCA.
- 2.1.2 Obligaciones de la AR.
- 2.1.3 Obligaciones del solicitante.
- 2.1.4 Obligaciones del suscriptor.
- 2.1.5 Obligaciones de los usuarios.
  - 2.1.5.1 Confianza en las firmas.
  - 2.1.5.2 Confianza en los Certificados.

**2.2 Responsabilidad.**

- 2.2.1 Responsabilidad de la CA.
- 2.2.2 Responsabilidad de la AR.
- 2.2.3 Responsabilidad del suscriptor.
- 2.2.4 Responsabilidad del usuario.

**2.3 Usos de los Certificados de IPSCA.****2.4 Interpretación y ejecución.**

- 2.4.1 Ley aplicable.
- 2.4.2 Subrogación, novación y notificaciones.
- 2.4.3 Procedimiento de resolución de conflictos.
- 2.4.4 Tasas de registro por la expedición y revocación de Certificados.

**2.5 Publicación y depósito.**

- 2.5.1 Publicación de la información de la CA.

- 2.6 Confidencialidad y protección de datos.**
  - 2.6.1 Confidencialidad de las claves de firma digital.
  - 2.6.2 Confidencialidad en la prestación de servicios de certificación.
  - 2.6.3 Protección de datos.
- 2.7 Derechos de Propiedad Intelectual.**
- 3 GESTIÓN DE LAS CLAVES.**
  - 3.1 Aspectos Generales.**
  - 3.2 Gestión de las claves de la CA.**
  - 3.3 Gestión de la claves del solicitante/suscriptor.**
- 4 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.**
  - 4.1 Supuestos de la revocación.**
    - 4.1.1 Efectos de la revocación.
  - 4.2 Supuestos de la suspensión.**
    - 4.2.1 Efectos y límites de la suspensión.
  - 4.3 Procedimiento de suspensión y revocación.**
    - 4.3.1 Legitimación activa.
    - 4.3.2 Recepción de solicitudes de suspensión/revocación.
    - 4.3.3 Decisión de suspender/revocar.
    - 4.3.4 Comunicación y publicación de la suspensión/revocación.
- 5 CADUCIDAD DE CERTIFICADOS.**
- 6 RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN.**
  - 6.1 Renovación de Certificados.**
    - 6.1.1 Requisitos previos.
- 7 EXTINCIÓN DE LA CA.**
- 8 CONTROLES DE SEGURIDAD.**
  - 8.1 Manual Interno de Seguridad.**
  - 8.2 Clasificación y control de activos.**
  - 8.3 Seguridad del Personal.**
  - 8.4 Seguridad física y del entorno.**
  - 8.5 Seguridad en la gestión de sistemas.**

**8.6 Plan de continuidad del negocio.**

**8.7 Cumplimiento.**

**9 CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS.**

**9.1 Características del Certificado.**

**9.2 Listas de Certificados.**

**10 OTRAS CUESTIONES.**

**10.1 Procedimientos de modificación de la CPS y de las Prácticas de Certificación.**

**10.2 Procedimiento de publicación de las modificaciones.**

**10.3 Procedimiento de notificación de las publicaciones.**

**11 Anexo I Políticas de Certificación de los Certificados Tipo B3**

**12 Anexo II Políticas de Certificación de los certificados tipo B3 Colegial**

**1.3 Identificación**

Esta CPS puede ser consultada por Internet en el servidor web de IPSCA, <http://www.ipsca.com>, o personalmente en las oficinas de IPSCA.

Todos los solicitantes y suscriptores de certificados manifiestan que conocen este documento, antes de la petición de cualquier tipo de certificado a IPSCA y además conocen el funcionamiento de los sistemas de clave pública en que se basan los certificados digitales.

Cualquier duda o consulta puede ser dirigida a IPSCA,

**IPS Certification Authority, S.L. (IPSCA)**  
**CIF B62210695**  
**Edificio ECU**  
**Ctra. De La Coruña, Km. 23,200**  
**28290 – Parque Rozas**  
**(Madrid)**  
**Tel. 91 640 20 52**  
**Fax 91 640 20 41**  
**general@ipsca.com**

## **1.4 Comunidad de usuarios y aplicabilidad**

### **1.4.1 Prestador del servicio de Certificación**

IPSCA actúa como Autoridad de Certificación (CA) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de un Certificado de conformidad con los términos de esta CPS y de la Política de Certificación (PC) de cada tipo de Certificado.

### **1.4.2 Autoridad de Registro**

IPSCA actúa como Autoridad de Registro y, comprobará, las identidades de los solicitantes de acuerdo a lo recogido en esta CPS.

IPSCA podrá delegar la comprobación de identidades en una o varias Autoridades de Registro. Las autoridades de registro comprobarán la identidad de los solicitantes de acuerdo con las normas de este CPS, la PC y el acuerdo de AR. La relación con las Autoridades de Registro se rige por acuerdos específicos de prestación de servicios.

### **1.4.3 Suscriptor**

El suscriptor será la persona física o jurídica a favor de la cual se ha emitido un Certificado Digital.

Los suscriptores deberán ajustarse a lo señalado en la CPS, en la PC del Certificado que han obtenido y, en su caso, en contrato de Prestación de Servicios suscrito con ipsCA

Los suscriptores deberán ajustarse a los procedimientos establecidos para la petición de cada clase y, en su caso, tipo de certificado, y cumplir los requisitos que se establezcan en esta CPS.

#### **1.4.4 Solicitante**

A los efectos de esta CPS, se entenderá por Solicitante a la persona física o jurídica, que actúa en nombre propio o en el de una persona jurídica a la que representa, y que está autorizada por cada una de las PC para presentar la solicitud de un Certificado.

#### **1.4.5 Usuario**

Se entiende por Usuario del Certificado a la persona que voluntariamente confía y hace uso de los Certificados de ipsCA. Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación el presente CPS.

## **1.5 Tipos de Certificados**

### **1.5.3. B1. Certificado de Correo con validez mensual/anual.**

En él se relaciona el nombre que introduzca en nuestro cuestionario con una cuenta de correo válida. Permite la firma y encriptación de correo.

No tiene carácter comercial pues no existe comprobación de la identidad del sujeto.

Toda la información contenida en el certificado es suministrada por la entidad que actúa como Autoridad de Registro bajo su entera responsabilidad, o por el propio usuario y resulta como información del suscriptor no verificada, de acuerdo con lo establecido en el presente CPS.

### **1.5.5. B3. Certificado Personal Presencial.**

ipsCA emite Certificados que permiten la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en esta CPS, en la PC de los Certificados Personales B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

La comprobación de la persona será presencial y documental. El individuo deberá presentarse ante la AR con un documento de identidad válido. LA AR puede ser un departamento de una empresa o cualquier otro tipo de Autoridad de Registro debidamente homologada por la CA

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la práctica oficial aplicable en función de la concreta Autoridad de Registro, y que debe consultarse en las Prácticas Certificación correspondientes.

### **1.5.6. B3. Colegial**

ipsCA emite Certificados que permiten la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor, su pertenencia a un Colegio profesional y con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en esta CPS, en la PC de los Certificados Personales B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

La comprobación de la persona será presencial y documental. El individuo deberá presentarse ante la AR con un documento de identidad válido. La AR será el colegio profesional para el que se emiten los certificados

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la práctica oficial aplicable en función de la concreta Autoridad de Registro, y que debe consultarse en las Prácticas Certificación correspondientes.

### **1.5.7 A1. Certificado de Servidor**

Los Certificados de Servidor de permiten incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta,

passwords, etc. Cobra especial importancia dentro del área del comercio electrónico, donde la seguridad de los datos es la principal lacra para el desarrollo de este sistema.

La emisión de un certificado de servidor implica tener registrado el dominio de Internet bajo el que se denomina el servidor y cumplir con el procedimiento que en el punto 3.3.5 se detalla.

## **1.6. Limitaciones de uso de los Certificados**

Los usos autorizados de los Certificados emitidos por la CA pueden estar especificados en cada tipo de certificado.

Las limitaciones de uso podrán ser de cualquier tipo y podrán venir establecidos tanto por la CA, como por el suscriptor o el usuario del certificado. Estas limitaciones quedarán reflejadas, asimismo, en el contrato que se suscriba entre la CA y el suscriptor o el usuario del certificado. En todo caso, las limitaciones de uso se deberán ajustar a la legislación vigente.

Sin perjuicio de las limitaciones de uso que se pudieran establecer, cabe la posibilidad de que se establezcan límites en el valor de las transacciones para las que puede utilizarse el certificado, con los mismos requisitos establecidos en la presente CPS para las limitaciones de uso

En todo caso un certificado puede contener o limitaciones de uso, o límites en el valor de las transacciones, o ambos aspectos, o ninguno de ellos.

## **1.7. Detalles de contacto**

**IPS Certification Authority, S.L. (IPSCA)**  
**CIF B62210695**  
**Edificio ECU**  
**Ctra. De La Coruña, Km. 23,200**  
**28290 – Parque Rozas**  
**(Madrid)**  
**Tel. 91 640 20 52**  
**Fax 91 640 20 41**  
**general@ipsca.com**

## **2. ASPECTOS GENERALES**

### **2.1 Obligaciones**

#### **2.1.1 Obligaciones de IPSCA**

- Emitir certificados conforme a esta CPS y a las PC correspondientes y a los estándares de aplicación.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente para los certificados.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos
- Mantener sus propias claves privadas bajo su exclusivo control empleando sistemas y productos fiables para almacenarlas de forma que garanticen su confidencialidad y los hagan inaccesibles a personas no autorizadas, evitando su pérdida o divulgación.
- Emitir los certificados solicitados ajustándose según lo dispuesto en la CPS, en las PC de cada tipo de Certificado y, en su caso, en los contratos de prestación de servicios de certificación correspondientes y en el Acuerdo para Autoridad de Registro.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica, y en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Facilitar el acceso a las versiones vigentes de la CPS y de las PC de cada tipo de Certificados.
- Ofrecer y mantener la infraestructura necesaria para los servicios de certificación, así como los controles de seguridad física, de procedimiento y personales necesarios para la práctica de la actividad de certificación.
- Aprobar o denegar las solicitudes de certificados.
- Poner copias de sus propios certificados y de cualquier información de revocación a disposición de quien desee verificar una firma digital con referencia a dichos certificados, para lo cual publicará en su servidor web <http://www.ipsca.com/crl/ipscab3crl2005.crl>. toda la información necesaria.
- Publicar los certificados emitidos respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

- Proteger los datos personales según requerimientos de la legislación sobre protección de datos de carácter personal
- Proporcionar al solicitante de la expedición del certificado la información mínima detallada en el artículo 18.b de la Ley 59/2003 de firma electrónica. Dicha información deberá transmitirse de forma gratuita, por escrito o por vía electrónica.
- Tomar medidas contra la falsificación de certificados y garantizar la confidencialidad de los datos de creación de firma durante el proceso de generación, así como su entrega por un procedimiento seguro al firmante.
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a esas condiciones de seguridad.
- No almacenar ni copiar los datos de creación de firma del Firmante.
- Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo. A estos efectos, el ipsCA almacena tanto en formato digital como en papel todas las versiones de la CPS publicadas y copia del "Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Clase B3". Igualmente, todos los certificados emitidos se almacenan en formato PKCS#7 (sin clave privada) con el fin de realizar, si llegara el caso, verificaciones de una firma efectuada con cualquiera de ellos.
- Informar sobre las modificaciones de esta Política y de su Declaración Prácticas de Certificación a los Subscriptores y AR's que estén vinculadas a ella.
- Cumplir las obligaciones del presente CPS y, en su caso, de la CPS de IPS.
- Todas aquellas obligaciones impuestas por la presente CPS y, en su caso, la Ley 59/2003 de firma electrónica, el Reglamento de firma electrónica, las leyes de protección de datos personales y por la normativa vigente.

### **2.1.2 Obligaciones de la AR**

La AR podrá asumir las siguientes obligaciones de las cuales será responsable.

- Identificar y autenticar correctamente al Suscriptor y/o Solicitante y/o a la organización que represente, conforme a los procedimientos que se establecen en esta CPS y en las Prácticas de Certificación específicas para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.
- Formalizar los contratos de expedición de Certificados con el Suscriptor en los términos y condiciones que establezca la CA.
- Almacenar de forma segura y por un periodo nunca inferior a 15 años la documentación aportada en el proceso de emisión del Certificado y en el proceso de suspensión / revocación del mismo, en los términos y condiciones que se establezcan en esta CPS, en la PC de cada tipo de certificados y, en su caso, en el acuerdo para la Autoridad de Registro
- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS y en la PC cada tipo de Certificado y, en su caso, el Acuerdo para Autoridad de Registro.

En todo caso, la AR permitirá a ipsCA el acceso a los archivos y a los procedimientos de conservación de los archivos asumidos por la AR y le dará el derecho a investigar cualquier sospecha de infracción de la CPS y/o de las PC por parte de la AR o cualquier poseedor de un Certificado. La AR y los poseedores de cualquier Certificado deberán informar a la ipsCA inmediatamente de cualquier sospecha de infracción.

IpsCA se reserva el derecho a asumir sin previo aviso cualquier parte de los servicios de certificación que preste la AR o a revocar o suspender cualquiera de los Certificados emitidos, si ello resulta necesario para preservar la seguridad del sistema de certificación.

### **2.1.3 Obligaciones del Solicitante**

- Abonar las tasas de registro que correspondan en virtud de los servicios que se soliciten.

- Suministrar a la AR la información necesaria para realizar una correcta identificación.
- Confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Solicitar el Certificado según se estipula en los términos y condiciones que se establezcan en la PC de cada tipo de Certificados y, en su caso, en el Contrato para la prestación de servicios de certificados suscrito con ipsCA.

#### **2.1.4 Obligaciones del Suscriptor**

- Conocer lo dispuesto en la presente CPS y en las PC del tipo de Certificado que posea, así como las modificaciones que se realicen sobre las mismas.
- •Abonar el precio y/o las tarifas correspondientes por la prestación de servicios de certificación de ipsCA.
- Conservar y utilizar correctamente el Certificado que se le entrega en concepto de depósito.
- Custodiar el Certificado, de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
- No realizar cualquier tipo de alteración en el Certificado, a través de cualquier tipo de medio y realizado por cualquier persona, excepto si dicha actividad está autorizada expresamente por la ley.
- Solicitar la suspensión o revocación del Certificado cuando se cumpla alguno de los supuestos previstos en los epígrafes que hacen referencia a la suspensión y revocación de certificados de la presente CPS.
- No revelar la clave privada ni el código de acceso del Certificado.
- Asegurarse de que toda la información contenida en el Certificado es cierta y notificar inmediatamente a ipsCA en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que, de forma sobrevenida, la información del Certificado no se corresponda con la realidad. Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir el Certificado, aunque éstos no estuvieran incluidos en el propio Certificado (tales como domicilio, nº de teléfono, etc.).

- Informar inmediatamente a ipsCA acerca de cualquier situación que pueda afectar a la validez del Certificado.
- No distribuir públicamente o transferir del Certificado, sin la previa autorización de ipsCA, a excepción de que sea necesario de acuerdo con lo establecido en la CPS, en las PC de cada tipo de Certificados y, en su caso, en el Contrato para la prestación de servicios de certificados suscrito con ipsCA.
- Destruir el Certificado cuando así lo exija ipsCA en virtud del derecho de propiedad que en todo caso conserva sobre el Certificado, cuando el Certificado caduque o sea revocado.
- Realizar un uso debido y correcto del Certificado, según se desprende de esta CPS y de las PC de cada Certificado. Será responsabilidad del Suscriptor el uso indebido que éste haga del mismo.
- Cualquier otra que se derive de la ley, del contenido de esta CPS, de la PC de cada tipo de Certificados y, en su caso, del Contrato para la prestación de servicios de certificados suscrito con ipsCA

### **2.1.5 Obligaciones de los Usuarios**

Los Usuarios que pretendan confiar y usar los Certificados emitidos por la CA deberán verificar la validez de las firmas emitidas por los Suscriptores.

En el supuesto de que los Usuarios no procedieran a verificar las firmas a través de la CRL (Lista de Certificados suspendidos o revocados), la ipsCA no se hace responsable del uso y confianza que los Usuarios hagan de estos Certificados.

#### **2.1.5.1 Confianza en las firmas**

Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un Certificado de IPSCA en la medida en que sea razonable hacerlo.

Para determinar si es razonable confiar, deberá tenerse en cuenta, en su caso, lo siguiente:

- La naturaleza de la operación correspondiente que la firma tenga por objeto avalar. No se considerará razonable confiar en una firma emitida por un certificado ipsCA si dicha operación puede ser considerada un uso indebido conforme a la lista adjunta.

- Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma, y en particular, si ha verificado que el certificado no esté caducado, suspendido o revocado. La caducidad constará en el propio Certificado. La posible suspensión o revocación del Certificado deberán ser consultadas en la lista de revocaciones o suspensiones de certificados (CRL).
- Si la parte que confía sabía o debía haber sabido que la firma estaba en entredicho o había sido revocada o suspendida.
- Las políticas y procedimientos que rijan la actividad de ipsCA con relación a las firmas emitidas mediante certificados por los emitidos y que se especifican en su CPS y en cada una de las Prácticas de Certificación emitidas para cada tipo de Certificado.
- Todo otro factor pertinente.

### **2.1.5.2 Confianza en los certificados**

Toda persona tendrá derecho a confiar en un Certificado IPSCA en la medida en que sea razonable hacerlo.

Para determinar si es razonable confiar, deberá tenerse en cuenta, en su caso, lo siguiente:

1. Toda restricción a que esté sujeto el certificado;
2. Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad del certificado, (CRL);
3. Las políticas y procedimientos que rijan la actividad del IPSCA con relación a las firmas emitidas mediante certificados por los emitidos y que se especifican en su CPS y en cada una de las Prácticas de Certificación emitidas para cada tipo de Certificado.
4. Todo otro factor pertinente.

Los usuarios del servicio de certificación IPSCA se obligan a conocer y aceptar los términos, condiciones y límites contenidos en esta CPS, en la CPS de IPS y en las PC específicas de su certificado, establecidas por contrato, dentro de los cuales se asegura la prestación de los servicios de certificación.

## **2.2 Responsabilidad**

### **2.2.1 Responsabilidad de la CA**

IPSCA, única y exclusivamente, responderá por los daños y perjuicios que causen a cualquier persona, cuando incumpla sus obligaciones legales derivadas de la legislación sobre firma electrónica o cuando actúe con negligencia en la prestación de servicios de certificación.

IPSCA no será responsable de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del Solicitante, Suscriptor y/o Usuario.

IPSCA no será responsable de la utilización negligente o dolosa de los Certificados y las claves.

IPSCA no será responsable de los daños y perjuicios que se deriven de actuaciones negligentes o dolosas por parte de terceros con relación a los certificados por ella emitidos en favor de un determinado suscriptor.

IPSCA no será responsable de las eventuales inexactitudes en el Certificado que resulten de la información facilitada por el Suscriptor, a condición de haber actuado siempre con la máxima diligencia exigible.

IPSCA no será responsable de los daños que se deriven de aquellas operaciones en que se hayan incumplido las limitaciones de uso que se señalan en las PC correspondientes a cada tipo de certificado.

IPSCA no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente CPS si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que IPSCA no pueda tener un control razonable.

IPSCA no será responsable del contenido de aquellos documentos electrónicos firmados digitalmente.

Ni IPSCA ni sus autoridades de registro serán responsables en ningún caso por los daños causados por el empleo de sus servicios de certificación pública en estos entornos.

### **2.2.2 Responsabilidad de la AR**

La AR responderá de las funciones que le correspondan conforme a esta CPS y, en especial, asumirá toda la responsabilidad por la correcta identificación y validación del

Solicitante/Suscriptor, con las mismas limitaciones que se establecen en el apartado anterior con relación a ipsCA.

La AR, responderá ante ipsCA por los daños y perjuicios que pudieran derivarse de la ejecución de esas funciones concertadas de manera negligente o en forma distinta a la contemplada en las presentes CPS y en las PC emitidas para cada tipo de Certificado.

No obstante, la AR no se hace responsable, en ningún caso, de la identidad o identificación del solicitante y/o suscriptor en el supuesto de falsificación de la documentación u otros datos aportados, por él mismo o por tercero que le suplantare.

### **2.2.3 Responsabilidad del Suscriptor**

El Suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta CPS.

El Suscriptor será responsable del cumplimiento de todas aquellas obligaciones impuestas por la presente CPS, las PC de cada tipo de Certificado, y por la normativa vigente en materia de prestación de servicios de certificación.

El Suscriptor se compromete a indemnizar a ipsCA los daños o perjuicios que puedan ocasionar cualquier acto u omisión culposo o doloso por su parte, asumiendo igualmente los gastos judiciales en que ipsCA pudiera incurrir por esta causa, incluyendo las costas de Abogados y Procuradores.

El suscriptor indemnizará y mantendrá indemne a ipsCA por cualquier daño que ésta pudiera sufrir por el cumplimiento total, parcial o defectuoso de las obligaciones asumidas por el suscriptor y en base a toda reclamación dirigida contra ella por cualquier tercero con el que el suscriptor hubiera contratado.

### **2.2.4 Responsabilidad del Usuario**

El Usuario será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta CPS.

El Usuario será responsable del cumplimiento de todas aquellas obligaciones impuestas por la presente CPS, las PC de cada tipo de Certificado, y por la normativa

vigente en materia de prestación de servicios de certificación.

En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado sin haber observado las obligaciones recogidas en la CPS y, en su caso, en las PC específicas de cada certificado, garantizando la plena indemnidad de ipsCA por dicho concepto.

### **2.3 Usos de los Certificados IPSCA**

Se considerará que se hace un uso indebido de un Certificado cuando éste sea utilizado para realizar operaciones no autorizadas según las Prácticas de Certificación aplicables a cada uno de los Certificados, el CPS y los Contratos de IPSCA con sus suscriptores.

Los productos, servicios, actividades o géneros cuya importación, exportación, circulación, tenencia, comercio o producción esté sometida a la adquisición de una autorización o licencia, o a una legislación especial, en cuyo caso, se regirá por la misma. Los productos, servicios, actividades o géneros adquiridos, realizados, producidos o comercializados de manera ilícita. En general, cualquier cosa considerada fuera del comercio.

### **2.4 Interpretación y ejecución**

#### **2.4.1 Ley aplicable**

El presente documento y las Prácticas de Certificación específicas para cada tipo de Certificado se regirán por la Ley española, con arreglo a la cual deberá ser interpretado su contenido.

#### **2.4.2 Subrogación, novación y notificaciones**

ipsCA se reserva el derecho de transmitir en el futuro todas las obligaciones y derechos que se deriven de este CPS a un tercero para que éste continúe prestando el servicio de certificación. En este caso, la CA notificará este extremo a los Suscriptores cuyos Certificados estén en vigor con una antelación mínima de dos meses, los cuales son conscientes y aceptan esta posibilidad. Esta CPS seguirá

siendo el documento que regule las relaciones entre las partes mientras no se cree un nuevo documento por escrito.

La CA podrá modificar cualquiera de las cláusulas de la presente CPS en los términos previstos en este CPS.

### **2.4.3 Procedimiento de resolución de conflictos**

Para la resolución de cualquier conflicto que pudiera surgir en relación a esta CPS o a las Prácticas de Certificación, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la Corte Española de Arbitraje.

### **2.4.4 Tasas de registro por la expedición y renovación de Certificados**

Las tasas de registro vigentes en cada momento por la expedición y renovación de Certificados serán puestas a disposición de los Solicitantes por cada AR. Estas últimas podrán, dentro del área en el que presten sus servicios, establecer promociones especiales, ofertas o similares que modifiquen las tarifas previamente establecidas.

## **2.5 Publicación y depósito**

### **2.5.1 Publicación de información de la CA**

El contenido de esta CPS, así como de toda la información que se publique, estará expuesta a título informativo en la dirección de Internet: <http://www.ipsca.com> y los originales estarán depositados en las oficinas de la CA.

Igualmente, tanto los Usuarios como los Solicitantes / Suscriptores podrán tener acceso de forma fiable a la información de la CA dirigiéndose a sus oficinas o a las de cualquier AR, o bien, solicitándolo a la dirección de correo [general@ipsca.com](mailto:general@ipsca.com) a través de la cual se remitirá la información firmada con un Certificado de IPSCA.

## **2.6 Confidencialidad y protección de datos**

### **2.6.1 Confidencialidad de las claves de firma digital**

ipsCA garantiza la confidencialidad frente a terceros durante el proceso de generación de las claves de firma criptográfica privadas que proporciona a sus clientes o que las Autoridades Certificadoras de Segundo Nivel encadenadas con IPSCA proporcionan a sus clientes. Asimismo, una vez generadas y entregadas las claves privadas, la CA se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves.

### **2.6.2 Confidencialidad en la prestación de servicios de certificación**

Tanto la CA como las AR mantendrán la más estricta confidencialidad de toda información recibida por los Solicitantes y Suscriptores de Certificados, siempre que la publicación o comunicación a terceros de dicha información no sea necesaria para la correcta prestación de los servicios de certificación. IpsCA solicitará la autorización de Solicitantes y Suscriptores cuando precise utilizar los datos para otros fines.

### **2.6.3 Protección de datos**

A los efectos de lo dispuesto en la normativa sobre tratamiento de datos de carácter personal, se informa al Suscriptor / Solicitante de la existencia de un fichero automatizado de datos de carácter personal creado y bajo la responsabilidad de IPSCA, con la finalidad de servir a los usos previstos en este CPS o cualquier otro relacionado con los servicios de certificación. El Suscriptor / Solicitante consiente expresamente la cesión de sus datos de carácter personal contenidos en dicho fichero, en la medida en que sea necesaria para llevar a cabo las acciones previstas en este CPS y en las Prácticas de Certificación.

El Responsable del fichero se compromete a poner los medios a su alcance para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal contenidos en el fichero. Cualquier otra utilización de los datos de carácter personal contenidos en el fichero, requerirá previo consentimiento del Suscriptor / Solicitante. Asimismo, se informa sobre el derecho que asiste al Suscriptor para acceder, rectificar o cancelar sus datos de carácter personal, en los términos recogidos por la normativa sobre tratamiento de datos de carácter personal.

## **2.7 Derechos de propiedad intelectual**

ipsCA es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS. Se prohíbe por

tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la CA sin la autorización expresa por su parte. No obstante, no necesitará autorización de ipsCA para la reproducción del Certificado cuando la misma sea necesaria para la utilización del Certificado por parte del usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta CPS, en la PC de cada certificado y, en su caso, en el contrato de Prestación de Servicio suscrito con ipsCA.

### **3. GESTIÓN DE LAS CLAVES:**

#### **3.1. Aspectos Generales:**

En general, ipsCA seguirá una serie de estándares o normas a la hora de generar el par de claves, como prestador de servicios de certificación. Estas normas o estándares son los siguientes:

- El tamaño de las claves será como mínimo de 1024 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- La generación de la función resumen (HASH) se realiza utilizando el algoritmo SHA1 de 160 bits
- El período de validez de las claves va a ser, como máximo, de cuatro años desde que se emite o renueva el Certificado, o el máximo establecido por la legislación vigente.

#### **3.2. Gestión de las Claves de la CA:**

Para la generación de las Claves de la CA de ipsCA se utilizó hardware. El estándar para el módulo criptográfico de generación de claves es el FIPS 140-2 nivel 2

Las claves de la CA se han mantenido depositadas offline y custodiadas en un sistema de Caja de Seguridad de una entidad especializada en almacenamiento seguro. El acceso a esas claves sólo se permite a dos personas debidamente autorizadas por IPSCA.

Existe una segunda copia de seguridad de la clave de la CA, dividida en dos partes almacenadas cada una de ellas de forma independiente y confidencial, fuera de las instalaciones de la CA.

En su caso, si en algún momento se viera en la necesidad de la eliminación de las claves, el procedimiento que se seguirá será el de sobre escritura.

## **4. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS**

La revocación y suspensión de Certificados son instrumentos a utilizar en el supuesto de que por alguna causa establecida en la presente CPS se deje de confiar en el Certificado antes de la finalización de su período de validez originalmente previsto.

### **4.1. Supuestos de revocación**

Los Certificados deberán ser revocados cuando concorra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Que se detecte que las claves privadas del Suscriptor o de la CA han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la AR, CA o el Suscriptor de las obligaciones establecidas en esta CPS.
- Por la resolución del contrato tal y como esta se regula en el apartado 8 de la presente CPS.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.

- Por la concurrencia de cualquier otra causa especificada en la presente CPS o en las correspondientes Prácticas de Certificación establecidas para cada tipo de Certificado.
- En el caso de los Certificados de Apoderados de Empresa, también será causa de revocación el cese del Representante de la Persona Jurídica representada.

#### **4.1.1. Efectos de la revocación**

El efecto de la revocación del Certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La revocación del Certificado por causa no imputable al Suscriptor originará la emisión de un nuevo Certificado a favor del Suscriptor por el plazo equivalente al restante para concluir el período originario de validez del Certificado revocado.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.

#### **4.2. Supuestos de suspensión**

El certificado podrá ser suspendido cuando existan indicios sobre la existencia de una causa de revocación. En la actualidad no se está proporcionando el servicio de suspensión debido a condicionantes técnicos, aunque se admite en este CPS a efectos de servicio futuro.

##### **4.2.1. Efectos y límites de la Suspensión**

El efecto de la suspensión de los Certificados es la pérdida de fiabilidad de los mismos, originando el cese temporal de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La suspensión de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La suspensión del Certificado terminará por cualquiera de las siguientes causas:

- Por la decisión de la CA de revocar el Certificado.  
Por decisión de la CA de levantar la suspensión del Certificado, una vez considerada la improcedencia de la revocación.
- Por la finalización anticipada del procedimiento de revocación.

### **4.3. Procedimiento de suspensión y revocación**

#### **4.3.1. Legitimación activa**

Deberán solicitar la suspensión/revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- El Suscriptor del Certificado así como la persona física o jurídica representada por éste.
- La AR, respecto a aquellos Certificados en cuya emisión hayan participado.
- La persona jurídica que conste en el Certificado.

Asimismo, podrá solicitar la suspensión/revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del Certificado.
- Fallecimiento del signatario.
- Incapacidad sobrevenida, total o parcial.
- Inexactitudes en el certificado.
- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.
- Cese del representante en el caso de los certificados con poderes.
- Extinción de la persona jurídica representada.
- Revocación de la autorización de la entidad que conste en el Certificado en el caso de los Certificados sin poderes.

En todo caso, la CA podrá iniciar de oficio el procedimiento de suspensión/revocación de Certificados, en cualquiera de los casos previstos en el apartado anterior.

La Autoridad judicial o administrativa podrá, en aquellos supuestos que marque la Ley 59/2003 de 19 de diciembre de firma electrónica, así como las demás disposiciones vigentes, instar a ipsCA a suspender/revocar el certificado.

#### **4.3.2. Recepción de solicitudes de suspensión/revocación**

La solicitud de suspensión/revocación de Certificados se podrá dirigir a la CA en la forma de comunicación escrita, personándose físicamente ante ipsCA o telefónicamente a través del siguiente número: +34 91 640.20.52

Aquel que solicite la suspensión/revocación deberá identificarse con una clave que le será suministrada junto con el certificado y que deberá guardar en lugar seguro, separada del propio certificado.

Las conversaciones telefónicas que se mantengan con la CA o la RA podrán ser grabadas y registradas por IPSCA a efectos probatorios.

Caso de no disponer de la clave, el suscriptor deberá desplazarse a un centro autorizado por la CA e identificarse, a fin de poder ejercitar su derecho de suspensión/revocación o solicitar la citada clave.

Cuando la persona que solicite la suspensión/revocación del certificado no sea el propio suscriptor, deberá dirigirse en persona a cualquiera de las oficinas de la CA o las AR.

#### **4.3.3. Decisión de suspender/revocar**

Una vez recibida y autenticada la solicitud de revocación, IPSCA procederá a tramitar la suspensión/revocación efectiva del Certificado. La decisión de suspender/revocar un Certificado corresponde a la CA.

#### **4.3.4. Comunicación y Publicación de la suspensión/revocación**

La decisión de revocar el Certificado será comunicada por ipsCA al Suscriptor mediante correo ordinario.

Igualmente, se publicará la revocación del Certificado en la CRL. La publicación de la CRL de ipcCA se realiza cada 24 horas o cada vez que se revoca un certificado.

Su consulta se puede realizar vía web en:

<http://www.ipsca.com/crl/ipscab3crl2005.crl>

La revocación surtirá efecto frente a terceros a partir de su publicación por parte de ipsCA, salvo que la causa de revocación sea el cese de la actividad de prestación de servicios de certificación de ipsCA, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

La información relativa al estado de la revocación estará disponible las 24 del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control ipsCA, ipsCA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

## **5. CADUCIDAD DE CERTIFICADOS**

Los Certificados caducarán por el transcurso del período operacional del mismo.

La caducidad producirá automáticamente la invalidez del Certificado, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La caducidad de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

## **6. RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN**

### **6.1. Renovación de Certificados**

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el suscriptor simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, la CA emitirá una nueva tarjeta y se generarán nuevas claves; pero, únicamente se van a llevar a cabo unas medidas mínimas de comprobación, puesto que el antiguo certificado tiene plena vigencia y nada hacer pensar, salvo que el suscriptor lo exprese, que alguno de sus datos ha cambiado o que ya no es posible confiar en el certificado.

Los certificados emitidos por IPSCA tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación si concurren las circunstancias recogidas en las PC de cada tipo de Certificados.

Los requisitos previos, la forma de solicitar la renovación y el procedimiento de renovación de certificados serán los que se especifiquen en las PC de cada Certificado.

## **7. EXTINCIÓN DE LA CA**

En orden a causar el menor daño posible tanto a los Suscriptores como a los Usuarios del sistema de certificación ante una hipotética desaparición de la CA se establecen las siguientes medidas:

- Comunicar la extinción mediante el envío de un correo electrónico certificado dirigido a todos los Suscriptores cuyos certificados permanezcan en vigor y la publicación de un anuncio en dos diarios de tirada nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

- Establecer, cuando ello fuera posible, acuerdos con terceras personas con la intención de transmitir todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, a la cual el Suscriptor da su consentimiento de manera expresa, esta CPS seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.
- Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otra entidad, a la revocación de todos los Certificados una vez transcurrido el plazo de dos meses desde la comunicación.
- Indemnizar adecuadamente a aquellos Suscriptores que lo soliciten cuando sus Certificados sean revocados con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el coste efectivo del servicio, descontando a prorrata el coste por los días transcurridos desde el inicio del contrato hasta la fecha de resolución.
- Cualquier otra obligación que venga impuesta por la ley.

## **8. CONTROLES DE SEGURIDAD**

### **8.1. Manual Interno de Seguridad**

Con el objeto de reforzar la seguridad técnica, física, de procedimientos y de capacitación del personal, la CA dispone de un Manual Interno de Seguridad que regula todos estos aspectos. Dicho Documento constituye parte de la documentación Interna de la empresa y, por lo tanto, forma parte del secreto de empresa, por lo que la integridad del mencionado manual no puede ser reproducida íntegramente en el presente CPS. No obstante, en este apartado del CPS procederemos a recoger las líneas maestras del Manual Interno de Seguridad.

Este manual de seguridad se entenderá como la política de seguridad de la información de IPSCA. Este Manual esta a disposición de todos los empleados que trabajan con sistemas de información.

Parte importante del Manual Interno de Seguridad será la organización de la Seguridad. Así, se definen roles y responsabilidades de seguridad para la

implementación de la seguridad de la información de IPSCA. Los roles definidos en el Manual de Seguridad son los siguientes:

- Gerente de Seguridad.
- Administrador de Seguridad.
- Gerente de Tecnologías de la Información (TI).
- Propietario del sistema.
- Propietario de la Información.
- Empleado de la empresa.

## **8.2. Clasificación y control de activos.**

ipsCA realiza un inventario de todo el hardware disponible para la generación de negocio y, en especial, ordenadores, impresoras y equipos de comunicaciones. En el mencionado inventario se especifica la marca, el modelo, el número de serie y otras cuestiones características del mencionado hardware. Además en el inventario se procede a recoger quien es el encargado del hardware.

ipsCA realiza un inventario de todo el software disponible para la generación de negocio y, en especial, de aquel hardware relacionado con su labor certificadora. En el mencionado inventario se especifica la versión, la fecha de la última actualización y, en general, todas aquellas cuestiones características del mismo. Además en el inventario se recoge quien es el usuario del mencionado software.

En el Manual de Seguridad se prevé la forma en que el inventario debe realizarse y la persona encargada de tal labor.

## **8.3. Seguridad del Personal.**

ipsCA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal cumple con los requisitos mínimos razonables para el desempeño de sus funciones. En concreto:

- a) ipsCA empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.
- b) Los roles de seguridad y responsabilidades especificadas en la política de seguridad de ipsCA, serán documentadas en la descripción del trabajo.
- c) Se deberá describir el trabajo del personal de ipsCA (temporal y fijo) desde el punto de vista de realizar una separación de tareas, definiendo los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones específicas de ipsCA.
- d) El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.
- e) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.
- f) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de ipsCA
- g) El personal de ipsCA será formalmente designado para desempeñar roles de confianza por el responsable de seguridad
- h) ipsCA no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.
- i) ipsCA no podrá asignar funciones que impliquen el manejo de elementos críticos del sistema a aquellas personas que no posean la experiencia necesaria en el propio ipsCA que propicie la confianza suficiente en el empleado. Se entenderá como

experiencia necesaria el haber pertenecido al Departamento en cuestión durante al menos 6 meses.

j) ipsCA debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de AC o AR, recibirá una formación relativa a:

- Los principales mecanismos de seguridad de AC y/o AR
- Todo el software de PKI y sus versiones empleados en el sistema de la AC
- Todas las tareas de PKI que se espera que realicen
- Los procedimientos de resolución de contingencias y continuidad de negocio

#### **8.4. Seguridad física y del entorno.**

IpsCA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados. En particular:

- a) El acceso físico a las instalaciones vinculadas a la generación de certificados, entrega del dispositivo al Firmante y servicios de gestión de revocaciones deberá ser limitado a las personas autorizadas y las instalaciones en las que se firman los certificados deberán ser protegidas de las amenazas físicas. La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la generación de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro. El acceso físico a las zonas de seguridad estará limitado al personal autorizado previa autenticación.
- b) Se establecerán controles para impedir la pérdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad
- c) Se establecerán controles para evitar el compromiso o robo de información
- d) Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de la AC sean sacados de las instalaciones sin autorización.

#### **8.5. Seguridad en la gestión de sistemas:**

ipsCA realiza periódicamente copias de seguridad de los datos que posee y, en especial, los relacionados con su labor certificadora.

ipsCA dispone de un registro de incidencias del equipo para el proceso de la información que alberga la CA de ipsCA.

ipsCA dispone de un procedimiento en el que se detalla el registro de usuarios y la gestión de permisos.

## **8.6. Plan de continuidad del negocio.**

IpsCA cuenta con un plan de continuidad del negocio para proteger los sistemas relacionados con la labor certificadora de ipsCA, de fallos o desastres. El mencionado plan establece un tiempo razonable de restauración, no superior a 48 horas, de las operaciones y de los sistemas informáticos relacionados con las funciones críticas de la labor certificadora de ipsCA, tras una interrupción, por cualquier motivo, de las funciones críticas de esta labor. El mencionado plan es comprobado regularmente y actualizado.

IpsCA notificará a todas las partes implicadas la interrupción de todo lo relacionado con su labor certificadora en el menor tiempo posible y cuando ipsCA tenga conocimiento del fallo o desastre que ha provocado la interrupción de su servicio de certificación. ipsCA notificará a todas las partes implicadas la restauración de su servicio de certificación, cuando así suceda.

## **8.7. Incidencias**

Incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos o al acceso de las distintas plataformas informáticas.

ipsCA cuenta con un procedimiento de notificación y gestión de incidencias. Todas las incidencias se comunican, según el procedimiento establecido, en el momento de producirse y quedarán almacenadas en un registro de incidencias. Mensualmente el registro de incidencias es revisado por un Responsable de ipsCA.

## **8.8. Cumplimiento.**

Todos los empleados que proceden al tratamiento de datos de carácter personal han recibido la formación y la información oportuna sobre las directrices marcadas por la legislación de protección de datos y las medidas que deben tener en cuenta cuando procedan al tratamiento de datos de carácter personal.

En cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, ipsCA ha elaborado e implementado un Documento de Seguridad.

## **9. CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS**

### **9.1. Características del Certificado**

Dependiendo del tipo de certificado, este podrá ser emitido en soporte de archivo de software o sobre tarjeta criptográfica. Las tarjetas serán emitidas tanto en las instalaciones donde se ubica la CA de ipsCA como en instalaciones externas, a partir de un fichero generado a tal efecto por ipsCA

Cuando las tarjetas sean grabadas y estampadas en instalaciones externas a ipsCA se proveerán los mecanismos de seguridad adecuados para que la información de las claves privadas de los usuarios no quede comprometida bajo ninguna circunstancia.

Los Certificados tendrán una validez establecida en el propio certificado y siempre acorde con la legislación vigente.

### **9.2. Listas de Certificados**

Los certificados una vez emitidos se publicarán en una base de datos o repositorio disponible públicamente. Esta operación será realizada por personal autorizado a partir de los ficheros generados por la ipsCA.

Los certificados revocados o suspendidos por ipsCA serán publicados en un repositorio público por parte del personal autorizado a partir de los ficheros generados por la ipsCA.

El Listado de Certificados en Vigor estará a disposición de los usuarios en la página web de ipsCA

El Listado de Certificados suspendidos o revocados (CRL) estará a disposición de los usuarios en la página <http://www.ipsca.com/crl/ipscab3crl2005.crl>

Los Certificados suspendidos y revocados aparecerán como tales en la CRL durante un período mínimo de tres años, a partir del cual se eliminará los datos del Certificado definitivamente de la CRL y serán depositados en las oficinas de la CA durante un

periodo de doce años.

Los Usuarios de Certificados pueden consultar en cualquier momento el estado de un Certificado determinado, bien visitando la página web, bien realizando la solicitud correspondiente a través del siguiente número de teléfono: +34 91 640.20.52

## **OTRAS CUESTIONES.**

### **9.3. Procedimientos de modificación de la CPS y de las Prácticas de Certificación.**

ipsCA podrá modificar las estipulaciones de la presente CPS y de sus PC, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y, siempre y cuando, toda modificación se justifique desde el punto de vista jurídico, técnico o comercial.

### **9.4. Procedimiento de publicación de las modificaciones.**

Las modificaciones efectuadas sobre la CPS o las Prácticas de Certificación se darán a conocer a los interesados en la página web de CA <http://www.ipsca.com> y en las oficinas de la CA y las AR.

### **9.5. Procedimiento de notificación de las publicaciones**

En caso que las modificaciones efectuadas en la CPS o en las Prácticas de Certificación incidan directamente en los derechos y obligaciones de los Suscriptores y/o Solicitantes, así como cuando dichas modificaciones alteren la operatividad de los Certificados por parte de los usuarios, deberán notificarse dichas modificaciones a los Suscriptores y/o Solicitantes con un período de antelación de quince días a la aplicación de los cambios efectuados.

El transcurso de dicho periodo sin que medie comunicación escrita por parte del Suscriptor y/o Solicitante, en contra de las citadas modificaciones implicará su aceptación. La no aceptación de las modificaciones de esta CPS o de las Prácticas de Certificación realizadas por la CA, tendrá como consecuencia la resolución de contrato

con el suscriptor/solicitante.

Se considerará como medio eficaz para la realización de notificaciones el correo electrónico firmado digitalmente y enviado a la dirección proporcionada por el Suscriptor y/o Solicitante.



---

18 de Mayo de 2005

**Políticas de Certificación (PC)  
Certificados Tipo B3**

---

**Anexo I**

**POLÍTICAS DE CERTIFICACIÓN  
De ipsCA**

**Certificados Tipo B3**

---

**IPS Certification Authority, s.l.**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52  
Fax 91 640 20 41  
general@ipsca.com  
<http://www.ipsca.com>

## **POLÍTICAS DE CERTIFICACIÓN**

**PC**

**Certificados Tipo B 3**

Versión 1.0

Fecha de Publicación: Mayo de 2005

PC de ipsCA

Todos los derechos reservados.

EL PRESENTE DOCUMENTO NO PUEDE SER REPRODUCIDO, DISTRIBUIDO, COMUNICADO PÚBLICAMENTE, ARCHIVADO O INTRODUCIDO EN UN SISTEMA DE RECUPERACIÓN DE INFORMACIÓN, O TRANSMITIDO, EN CUALQUIER FORMA Y POR CUALQUIER MEDIO (ELECTRÓNICO, MECÁNICO, FOTOGRÁFICO, GRABACIÓN O CUALQUIER OTRO), TOTAL O PARCIALMENTE, SIN EL PREVIO CONSENTIMIENTO POR ESCRITO DE ipsCA.

**IPS Certification Authority, s.l.**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52  
Fax 91 640 20 41  
general@ipsca.com  
<http://www.ipsca.com>

**1.- ÍNDICE:**

<b><u>2.- DEFINICIONES:</u></b> .....	<b>3</b>
<b><u>3.- INTRODUCCIÓN:</u></b> .....	<b>5</b>
<b><u>3.1.- Presentación:</u></b> .....	<b>5</b>
<b><u>3.2. Estructura:</u></b> .....	<b>5</b>
<b><u>3.3 Identificación:</u></b> .....	<b>6</b>
<b><u>3.4 .- Detalles de contacto:</u></b> .....	<b>6</b>
<b><u>4.- COMUNIDAD DE USUARIOS Y APLICABILIDAD:</u></b> .....	<b>7</b>
<b><u>4.1.- Prestador de Servicios de Certificación:</u></b> .....	<b>7</b>
<b><u>4.2.- Autoridad de Registro:</u></b> .....	<b>7</b>
<b><u>4.3.- Solicitante:</u></b> .....	<b>7</b>
<b><u>4.4.- Suscriptor:</u></b> .....	<b>7</b>
<b><u>4.5.- Usuario:</u></b> .....	<b>7</b>
<b><u>5.- CERTIFICADOS EMITIDOS POR ipsCA:</u></b> .....	<b>8</b>
<b><u>5.1.- Certificados TIPO B3:</u></b> .....	<b>8</b>
<b><u>6.- CERTIFICADOS TIPO B3:</u></b> .....	<b>9</b>
<b><u>6.1.- Aspectos Generales:</u></b> .....	<b>9</b>
<b><u>6.1.1.- Ámbito de aplicación:</u></b> .....	<b>9</b>
<b><u>6.1.2.- Datos incluidos en el Certificado:</u></b> .....	<b>9</b>
<b><u>6.1.3.- Usos del Certificado y sus límites:</u></b> .....	<b>11</b>
<b><u>6.1.4.- Generación de las Claves y del Certificado:</u></b> .....	<b>13</b>
<b><u>6.2.- Solicitud del Certificado:</u></b> .....	<b>13</b>
<b><u>6.2.1.- Requisitos del Solicitante:</u></b> .....	<b>13</b>
<b><u>6.2.2.- Procedimiento de Solicitud, identificación y autenticación y emisión:</u></b> ..	<b>14</b>
<b><u>6.3.- Revocación del Certificado:</u></b> .....	<b>16</b>
<b><u>6.3.1.- Supuestos de revocación:</u></b> .....	<b>16</b>
<b><u>6.3.2.- Efectos de la revocación:</u></b> .....	<b>17</b>
<b><u>6.3.3.- Procedimiento de revocación:</u></b> .....	<b>17</b>
<b><u>6.4.- Renovación del Certificado:</u></b> .....	<b>19</b>
<b><u>6.5.- Validez del Certificado:</u></b> .....	<b>19</b>

## 2.- DEFINICIONES:

- **Acuerdo de Autoridad de Registro:** Contrato suscrito entre ipsCA y una determinada persona física o jurídica, que tiene como objeto regular la relación jurídica entre ambos para una correcta comprobación de identidades para la emisión de Certificados Digitales por parte de ipsCA
- **Autoridad de Registro (AR):** Persona física o jurídica encargada de la comprobación de identidades para la emisión de Certificados Digitales por parte de ipsCA
- **Autoridad de Registro (AR) delegada:** Autoridad de Registro (AR)
- **Certificado (Certificado Digital):** Documento electrónico firmado digitalmente por ipsCA que vincula una clave pública con una determinada persona (física o jurídica) y que tiene como principal finalidad confirmar la identidad de la mencionada persona.
- **Clave Privada:** Clave criptográfica única que el suscriptor utiliza para crear una firma electrónica.
- **Clave Pública:** Clave criptográfica única vinculada a la clave privada que es utilizada para verificar la firma electrónica creada por la clave privada.
- **Contrato de Prestación de Servicios de Certificación:** Contrato que tiene por objeto regular los derechos y obligaciones derivados de la prestación por ipsCA, al suscriptor, de los servicios de Certificación, y, en su caso, la revocación y renovación, del mencionado servicio de Certificación.
- **CRL:** Certificado que tiene por objeto recoger los certificados emitidos y, en su caso, revocados por ipsCA
- **Declaración de Prácticas de Certificación (CPS):** Documento actualizado en el que ipsCA especifica los aspectos más relevantes de la gestión del ciclo de vida de los certificados, incluyendo, aunque no limitado, las condiciones para la solicitud, emisión, uso y revocación de los certificados de ipsCA

- **Documento de identidad válido:** Documento Nacional de Identidad, Pasaporte y demás documentos que la legislación española admita como válidos para acreditar la identidad de una persona.
- **Fedatario Público:** Persona encargada de emitir documentos públicos de acuerdo con las solemnidades requeridas por la legislación española.
- **Firma Electrónica:** Conjunto de datos electrónicos asociados a otros datos electrónicos y vinculados únicamente al suscriptor de un certificado, permitiendo su identificación y que ha sido creada por medios que éste puede tener bajo su exclusivo control y está vinculada a los datos a los que se refiere, lo que permite detectar cualquier modificación posterior de éstos.
- **Políticas de Certificación (PC):** Documento actualizado en el que ipsCA especifica un conjunto de reglas que señalan los procedimientos seguidos por ipsCA en relación a la solicitud, identificación y revocación de un certificado, así como los límites de uso, el ámbito de aplicación y las características técnicas de cada tipo de certificado.
- **Prestador de Servicios de Certificación:** Persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica.
- **Solicitante:** Persona física o jurídica, que actúa en nombre propio o en el de una persona jurídica a la que representa, y que está autorizada, en función de cada una de las PC de cada Certificado, a solicitar un Certificado Digital.
- **Suscriptor:** Persona física o jurídica a favor de la cual se ha emitido un Certificado Digital y que posee un Certificado y lo utiliza de acuerdo con las Políticas de Certificación.
- **Usuario:** Persona que voluntariamente confía y hace uso de los Certificados de ipsCA

### **3.- INTRODUCCIÓN**

#### **3.1.- Presentación**

El presente documento recoge la Política de Certificación (PC) de ipsCA para los Certificados Personales Tipo B3. Esta PC pormenoriza y completa lo establecido en la CPS de ipsCA, recogiendo un conjunto de reglas que indican los procedimientos seguidos por ipsCA en la prestación de sus servicios (solicitud, identificación, aceptación y revocación) así como los límites de uso, el ámbito de aplicación y las características técnicas de este tipo de certificado.

Esta Política de Certificación (PC), junto con la CPS de ipsCA, están dirigida a cualquiera que confíe de buena fe en este tipo de certificados.

#### **3.2. Estructura**

La estructura de esta PC es la siguiente:

- 1 ÍNDICE**
- 2 DEFINICIONES**
- 3 INTRODUCCIÓN**
  - 3.1 Presentación**
  - 3.2 Estructura**
  - 3.3 Identificación**
  - 3.4 Detalles de contacto**
- 4 COMUNIDAD DE USUARIOS Y APLICABILIDAD**
  - 4.1 Prestador de Servicios de certificación**
  - 4.2 Autoridad de Registro**
  - 4.3 Solicitante**
  - 4.4 Suscriptor**
  - 4.5 Usuario**
- 5 CERTIFICADOS EMITIDOS POR ipsCA**
  - 5.1 Certificados Clase 3**
- 6 CERTIFICADOS TIPO B3**
  - 6.1 Aspectos Generales**
    - 6.1.1 Ámbito de Aplicación**

- 6.1.2 Datos incluidos en el Certificado**
- 6.1.3 Usos del Certificado y sus límites**
- 6.1.4 Generación de las Claves y del Certificado**
- 6.2 Solicitud del Certificado**
  - 6.2.1 Requisitos del Solicitante**
  - 6.2.2 Procedimiento de Solicitud, identificación y autenticación y emisión**
- 6.3 Revocación del Certificado**
  - 6.3.1 Supuestos de revocación**
  - 6.3.2 Efectos de la revocación**
  - 6.3.3 Procedimiento de revocación**
- 6.4 Renovación del Certificado**
  - 6.4.1. Requisitos previos**
  - 6.4.2. Cómo solicitar la renovación**
  - 6.4.3 Procedimiento de renovación**
- 6.5 Validez del Certificado**
- 6.6 Aceptación de Certificados**

### **3.3 Identificación**

Estas PC puede ser consultada por Internet en el servidor web de ipsCA, <http://www.ipsca.com> o personalmente en las oficinas de ipsCA.

Todos los solicitantes y suscriptores de certificados manifiestan que conocen este documento, antes de la petición de cualquier tipo de certificado a ipsCA y además conocen el funcionamiento de los sistemas de clave pública en que se basan los certificados digitales.

### **3.4 .- Detalles de contacto**

#### **IPS Certification Authority, s.l.**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52

## **4.- COMUNIDAD DE USUARIOS Y APLICABILIDAD**

#### **4.1.- Prestador de Servicios de Certificación**

ipsCA actúa como Autoridad Certificadora (CA) relacionando una determinada clave pública con un sujeto, entidad o sitio Web concretos a través de la emisión de un Certificado de conformidad con los términos de estas PC y con el CPS de ipsCA.

#### **4.2.- Autoridad de Registro**

ipsCA delega la comprobación de identidades en una o varias Autoridades de Registro (AR). Esta delegación se formalizará en un Acuerdo para Autoridad de Registro. Las autoridades de registro delegadas deberán comprobar la identidad de los solicitantes de acuerdo con las normas de estas PC, de la CPS y del Acuerdo para Autoridad de Registro.

#### **4.3.- Solicitante**

A los efectos de estas PC, se entenderá por Solicitante a la persona física o jurídica, que actúa en nombre propio o en el de una persona jurídica a la que representa, y que está autorizada, en función de cada una de las PC de cada Certificado, que se detallan más adelante, a solicitar un Certificado Digital..

#### **4.4.- Suscriptor**

El suscriptor será la persona física o jurídica a favor de la cual se ha emitido un Certificado Digital.

Los suscriptores deberán ajustarse a lo señalado en las PC, en la CPS y, en su caso, en contrato de Prestación de Servicios suscrito con ipsCA.

#### **4.5.- Usuario**

Se entiende por Usuario del Certificado a la persona que voluntariamente confía y hace uso de los Certificados de ipsCA.

Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación las presentes PC, así como la CPS.

## **5.- CERTIFICADOS EMITIDOS POR ipsCA:**

### **5.1.- B1. Certificado de Correo con validez mensual/anual.**

En él se relaciona el nombre que introduzca en nuestro cuestionario con una cuenta de correo válida. Permite la firma y encriptación de correo.

No tiene carácter comercial pues no existe comprobación de la identidad del sujeto.

Toda la información contenida en el certificado es suministrada por la entidad que actúa como Autoridad de Registro bajo su entera responsabilidad, o por el propio usuario y resulta como información del suscriptor no verificada, de acuerdo con lo establecido en el CPS de ipsCA.

### **5.2. B3. Certificado Personal Presencial.**

ipsCA emite Certificados que permiten la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en esta CPS, en la PC de los Certificados Personales B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

La comprobación de la persona será presencial y documental. El individuo deberá presentarse ante la AR con un documento de identidad válido. LA AR puede ser un departamento de una empresa o cualquier otro tipo de Autoridad de Registro debidamente homologada por la CA

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la práctica oficial aplicable en función de la concreta Autoridad de Registro, y que debe consultarse en las Prácticas Certificación correspondientes.

### **5.3. B3. Colegial**

ipsCA emite Certificados que permiten la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor, su pertenencia a un Colegio profesional y con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en esta CPS, en la PC de los Certificados Personales B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

La comprobación de la persona será presencial y documental. El individuo deberá presentarse ante la AR con un documento de identidad válido. La AR será el colegio profesional para el que se emiten los certificados

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la práctica oficial aplicable en función de la concreta Autoridad de Registro, y que debe consultarse en las Prácticas Certificación correspondientes.

### **5.4 A1. Certificado de Servidor**

Los Certificados de Servidor de permiten incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta, passwords, etc. Cobra especial importancia dentro del área del comercio electrónico, donde la seguridad de los datos es la principal lacra para el desarrollo de este sistema.

La emisión de un certificado de servidor implica tener registrado el dominio de Internet bajo el que se denomina el servidor y cumplir con el procedimiento que en el punto 3.3.5 se detalla.

ipsCA emite Certificados que posibilitan la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en la CPS, en esta PC de los Certificados Tipo B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

## 6.- CERTIFICADOS TIPO B3

### 6.1.- Aspectos Generales:

#### 6.1.1.- Ámbito de aplicación:

En este tipo de Certificados se relaciona la identidad de un suscriptor con su clave pública y permite la firma de documentos electrónicos.

Por ello les será de aplicación las normas españolas referidas a la firma electrónica y, especialmente, la Ley 59/2003 de 19 de diciembre de firma electrónica

#### 6.1.2.- Datos incluidos en el Certificado:

Los datos que se incluirán en un Certificado Clase 3 Reconocido emitido por ipsCA serán los siguientes:

#### Asunto:

CN= "NOMBRE" blanco *NOMBRE* blanco 1<sup>er</sup> *APELLIDO* blanco 2º *APELLIDO* blanco "–  
" blanco "NIF" blanco *NIF CON 9 DIGITOS*

OU= *DEPARTAMENTO*

O= *EMPRESA*

L= Localidad donde se encuentre empadronado el suscriptor

S= Provincia donde se encuentre empadronado el suscriptor

C="ES"

E= Dirección de correo electrónico del suscriptor

#### Extensiones estándar

#### Extensiones especiales

Se incluye el parseo de un Certificado Tipo B3 de prueba:

0:d=0 hl=4 l=1417 cons: SEQUENCE  
4:d=1 hl=4 l=1137 cons: SEQUENCE  
8:d=2 hl=2 l= 3 cons: cont [ 0 ]  
10:d=3 hl=2 l= 1 prim: INTEGER :02  
13:d=2 hl=2 l= 10 prim: INTEGER :1285EA01000000000152  
25:d=2 hl=2 l= 13 cons: SEQUENCE  
27:d=3 hl=2 l= 9 prim: OBJECT :sha1WithRSAEncryption  
38:d=3 hl=2 l= 0 prim: NULL  
40:d=2 hl=3 l= 183 cons: SEQUENCE  
43:d=3 hl=2 l= 11 cons: SET  
45:d=4 hl=2 l= 9 cons: SEQUENCE  
47:d=5 hl=2 l= 3 prim: OBJECT :countryName  
52:d=5 hl=2 l= 2 prim: PRINTABLESTRING :ES  
56:d=3 hl=2 l= 18 cons: SET  
58:d=4 hl=2 l= 16 cons: SEQUENCE  
60:d=5 hl=2 l= 3 prim: OBJECT :stateOrProvinceName  
65:d=5 hl=2 l= 9 prim: PRINTABLESTRING :Barcelona  
76:d=3 hl=2 l= 18 cons: SET  
78:d=4 hl=2 l= 16 cons: SEQUENCE  
80:d=5 hl=2 l= 3 prim: OBJECT :localityName  
85:d=5 hl=2 l= 9 prim: PRINTABLESTRING :Barcelona  
96:d=3 hl=2 l= 25 cons: SET  
98:d=4 hl=2 l= 23 cons: SEQUENCE  
100:d=5 hl=2 l= 3 prim: OBJECT :organizationName  
105:d=5 hl=2 l= 16 prim: PRINTABLESTRING :IPS Seguridad CA  
123:d=3 hl=2 l= 24 cons: SET  
125:d=4 hl=2 l= 22 cons: SEQUENCE  
127:d=5 hl=2 l= 3 prim: OBJECT :organizationalUnitName  
132:d=5 hl=2 l= 15 prim: PRINTABLESTRING :Certificaciones  
149:d=3 hl=2 l= 43 cons: SET  
151:d=4 hl=2 l= 41 cons: SEQUENCE  
153:d=5 hl=2 l= 3 prim: OBJECT :commonName  
158:d=5 hl=2 l= 34 prim: PRINTABLESTRING :CLASE B-3 ipsCA-IPS Seguridad  
2005  
194:d=3 hl=2 l= 30 cons: SET  
196:d=4 hl=2 l= 28 cons: SEQUENCE  
198:d=5 hl=2 l= 9 prim: OBJECT :emailAddress

209:d=5 hl=2 l= 15 prim: IA5STRING :ips@mail.ips.es  
226:d=2 hl=2 l= 30 cons: SEQUENCE  
228:d=3 hl=2 l= 13 prim: UTCTIME :050525114712Z  
243:d=3 hl=2 l= 13 prim: UTCTIME :070525115712Z  
258:d=2 hl=3 l= 192 cons: SEQUENCE  
261:d=3 hl=2 l= 36 cons: SET  
263:d=4 hl=2 l= 34 cons: SEQUENCE  
265:d=5 hl=2 l= 9 prim: OBJECT :emailAddress  
276:d=5 hl=2 l= 21 prim: IA5STRING :DIRECCION @CORREO.COM  
299:d=3 hl=2 l= 11 cons: SET  
301:d=4 hl=2 l= 9 cons: SEQUENCE  
303:d=5 hl=2 l= 3 prim: OBJECT :countryName  
308:d=5 hl=2 l= 2 prim: PRINTABLESTRING :ES  
312:d=3 hl=2 l= 18 cons: SET  
314:d=4 hl=2 l= 16 cons: SEQUENCE  
316:d=5 hl=2 l= 3 prim: OBJECT :stateOrProvinceName  
321:d=5 hl=2 l= 9 prim: PRINTABLESTRING :PROVINCIA  
332:d=3 hl=2 l= 15 cons: SET  
334:d=4 hl=2 l= 13 cons: SEQUENCE  
336:d=5 hl=2 l= 3 prim: OBJECT :localityName  
341:d=5 hl=2 l= 6 prim: PRINTABLESTRING :CIUDAD  
349:d=3 hl=2 l= 16 cons: SET  
351:d=4 hl=2 l= 14 cons: SEQUENCE  
353:d=5 hl=2 l= 3 prim: OBJECT :organizationName  
358:d=5 hl=2 l= 7 prim: PRINTABLESTRING :EMPRESA  
367:d=3 hl=2 l= 21 cons: SET  
369:d=4 hl=2 l= 19 cons: SEQUENCE  
371:d=5 hl=2 l= 3 prim: OBJECT :organizationalUnitName  
376:d=5 hl=2 l= 12 prim: PRINTABLESTRING :DEPARTAMENTO  
390:d=3 hl=2 l= 61 cons: SET  
392:d=4 hl=2 l= 59 cons: SEQUENCE  
394:d=5 hl=2 l= 3 prim: OBJECT :commonName  
399:d=5 hl=2 l= 52 prim: PRINTABLESTRING :NOMBRE RECONOCIDO PRUEBA  
CERTIFICADO - NIF 00000000Z  
453:d=2 hl=3 l= 159 cons: SEQUENCE  
456:d=3 hl=2 l= 13 cons: SEQUENCE  
458:d=4 hl=2 l= 9 prim: OBJECT :rsaEncryption

469:d=4 hl=2 l= 0 prim: NULL  
471:d=3 hl=3 l= 141 prim: BIT STRING  
615:d=2 hl=4 l= 526 cons: cont [ 3 ]  
619:d=3 hl=4 l= 522 cons: SEQUENCE  
623:d=4 hl=2 l= 14 cons: SEQUENCE  
625:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Key Usage  
630:d=5 hl=2 l= 1 prim: BOOLEAN :255  
633:d=5 hl=2 l= 4 prim: OCTET STRING  
639:d=4 hl=2 l= 29 cons: SEQUENCE  
641:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Extended Key Usage  
646:d=5 hl=2 l= 22 prim: OCTET STRING  
670:d=4 hl=2 l= 29 cons: SEQUENCE  
672:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Subject Key Identifier  
677:d=5 hl=2 l= 22 prim: OCTET STRING  
701:d=4 hl=3 l= 210 cons: SEQUENCE  
704:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Authority Key Identifier  
709:d=5 hl=3 l= 202 prim: OCTET STRING  
914:d=4 hl=2 l= 108 cons: SEQUENCE  
916:d=5 hl=2 l= 3 prim: OBJECT :X509v3 CRL Distribution Points  
921:d=5 hl=2 l= 101 prim: OCTET STRING  
1024:d=4 hl=2 l= 119 cons: SEQUENCE  
1026:d=5 hl=2 l= 8 prim: OBJECT :Authority Information Access  
1036:d=5 hl=2 l= 107 prim: OCTET STRING  
1145:d=1 hl=2 l= 13 cons: SEQUENCE  
1147:d=2 hl=2 l= 9 prim: OBJECT :sha1WithRSAEncryption  
1158:d=2 hl=2 l= 0 prim: NULL  
1160:d=1 hl=4 l= 257 prim: BIT STRING

### 6.1.3.- Usos del Certificado y sus límites:

Este tipo de Certificado se utilizará, principalmente, para firmar electrónicamente, documentos electrónicos Con este hecho se garantiza:

*Identificación del firmante* El Firmante del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.

*Integridad del documento firmado:* La utilización de este Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante. Se certifica que el mensaje recibido por el Tercero que confía es el mismo que fue emitido por el Firmante

*No repudio de origen:* Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Firmante que ha firmado no puede negar la autoría o la integridad del mismo.

Este Certificado se podrá utilizar, para la firma de mensajes de correo electrónico que soporten protocolo S/MIME y para la autenticación en servidores web seguros utilizando el protocolo SSL 3.0

Por las características esenciales del certificado éste podría ser utilizado para otras finalidades y, en concreto, para el cifrado y descifrado de documentos o mensajes electrónicos. No obstante, este uso es de exclusiva responsabilidad del suscriptor y/o el usuario del certificado, ipsCA no asume ningún tipo de responsabilidad, ya sea legal, contractual o extra contractual, derivada de daños directos o indirectos por la utilización del certificado para tal finalidad, debido a que, por motivos de seguridad, esta Política determina que ipsCA no guarde copia de la clave privada del Firmante.

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso.

El empleo de los certificados que implique la realización de operaciones no autorizadas según las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los Contratos de ipsCA con sus Firmantes tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto ipsCA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el Firmante o cualquier tercero.

En función de los servicios prestados por ipsCA mediante la emisión de sus certificados, no es posible por parte de ipsCA el acceso o conocimiento del contenido del mensaje al que haya sido adjuntado o con el que se relacione el uso de un certificado emitido por ipsCA. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de ipsCA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el signatario cualquier responsabilidad dimanante del contenido de

dicho mensaje aparejado al uso de un certificado emitido por ipsCA.

Asimismo, le será imputable al signatario cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los contratos de ipsCA con sus Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación española vigente sobre firma electrónica

#### 6.1.4.- Generación de las Claves y del Certificado:

El soporte para el almacenamiento de las claves y el certificado será siempre:

Un tarjeta o dispositivo criptográfico. El acceso al dispositivo criptográfico, donde se encuentra la clave privada, se realizará a través de contraseña (PIN). Para realizar una firma electrónica es necesario introducir el PIN que únicamente debe conocer el subscriptor. En la generación de las claves no se permite realizar una copia de seguridad de las mismas.

#### 6.2.- Solicitud del Certificado:

##### 6.2.1.- Requisitos del Solicitante:

Para ser solicitante y, en su caso y posteriormente, ser suscriptor de este tipo de certificados, es necesario cumplir con estos requisitos:

Ser persona física

Poseer un Documento de identidad válido.

##### 6.2.2.- Procedimiento de Solicitud, identificación y autenticación y emisión:

El usuario se presentará ante la AR y acreditará su identidad mostrando a la AR un Documento de Identidad válido.

Todos los Firmantes requieren un nombre distintivo (DN o distinguished name)

conforme al estándar X.500. Los pseudónimos no serán admitidos.

Tras autenticar al usuario y comprobar los datos el ipsCA emitirá el certificado y se lo entregará de manera segura al usuario.

## Emisión

1. El operador de la CA introduce en el lector de tarjetas o el dispositivo criptográfico, que está conectado al módulo de emisión y validación de certificados, la tarjeta o dispositivo preimpresa del solicitante.

2. El módulo de validación y emisión de Certificados ejecuta las siguientes operaciones:  
Genera automáticamente las claves (pública y privada) en la propia tarjeta o dispositivo criptográfico.

Envía el CSR (Petición de certificado) a la CA donde se firmará en modo automático.

El certificado es devuelto por la CA e instalado en la tarjeta o dispositivo.

3. La tarjeta o dispositivo criptográfico dispone de un PIN de acceso conocido por defecto cuando aún no contiene un certificado. El módulo de validación y emisión de Certificados introduce el PIN por defecto de manera automática, para acceder a la tarjeta. Tras instalar el certificado emitido, genera un PIN aleatorio basado en una combinación de 10 dígitos alfanuméricos que introduce en la tarjeta criptográfica.

Nota: En ningún momento del proceso, el operador de la CA tiene acceso al PIN aleatorio generado por el módulo de emisión. De esta manera, se garantiza que la firma electrónica generada cumple los requisitos para ser considerada firma electrónica avanzada según el artículo 3.2 de la LFE al ser solo el suscriptor de la firma el que conoce el PIN de acceso a la tarjeta criptográfica.

4. La aplicación genera automáticamente una carta en papel autocopiativo inverso conteniendo el PIN impreso para su envío por correo postal al suscriptor de la firma. Además se imprimen tres copias del "Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA, personalizado con los datos del Certificado y del solicitante.

5. Se remite al domicilio del solicitante el PIN definitivo

6. La Tarjeta que contiene el Certificado, junto con las tres copias del documento antes mencionado se remiten a la AR.

### Entrega

Una vez que el usuario ha recibido la carta con el PIN, debe acudir personalmente a la AR en un plazo de 30 días. Queda totalmente prohibida la asistencia en nombre o representación de otra persona.

El solicitante debe aportar a la AR su DNI o pasaporte para demostrar su identidad.

Si el solicitante no acude en el mencionado plazo a la AR, se procede a la revocación del certificado y la devolución ipsCA del soporte que lo contenga donde se destruye físicamente

El operador de la AR comprueba que los datos incluidos en el DNI coinciden con los datos impresos en la tarjeta criptográfica y que coinciden, además, con los del “Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA

El solicitante debe comprobar en la propia AR que los datos del certificado son correctos y se corresponden con los suyos.

El agente autorizado para la verificación de identidad de la AR y el solicitante deben firmar las tres copias del documento “Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA

El agente autorizado para la verificación de identidad de la AR archiva una copia firmada del “Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA”, entregará al solicitante otra de las copias firmadas junto con el certificado soportado en tarjeta o dispositivo criptográfico y la tercera copia será remitida en un plazo no superior a siete días ipsCA

### **6.3.- Revocación del Certificado:**

### **6.3.1.- Supuestos de revocación:**

Los Certificados Tipo B3 deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor.
- Pérdida o inutilización por daños del soporte del certificado o modificación del certificado.
- Utilización indebida del certificado por el suscriptor o por terceros.
- Fallecimiento del suscriptor.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Por error en la emisión del certificado debido a una no adecuación al procedimiento establecido en las PC establecidas para los Certificados Tipo B3 y/o, en su caso, en el contrato establecido entre ipsCA y el suscriptor.
- Que se detecte que las claves privadas del Suscriptor o de ipsCA han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la AR, ipsCA o el Suscriptor de las obligaciones establecidas en la CPS.
- Por la resolución del contrato.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la CPS o en las presentes PC establecidas para cada tipo de Certificado.

En cualquier caso, todas las solicitudes deberán ser autenticadas.

### 6.3.2.- Efectos de la revocación

El efecto de la revocación del Certificado Clase 3 es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La revocación del Certificado por causa no imputable al Suscriptor originará la emisión de un nuevo Certificado a favor del Suscriptor por el plazo equivalente al restante para concluir el período originario de validez del Certificado revocado.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.

### 6.3.3.- Procedimiento de revocación:

Deberán solicitar la revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- El Suscriptor del Certificado TIPO B3.
- La AR, respecto a aquellos Certificados en cuya emisión hayan participado.

Asimismo, podrá solicitar la revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del Certificado.
- Fallecimiento del suscriptor.
- Incapacidad sobrevenida, total o parcial.
- Inexactitudes en el certificado.
- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.

En todo caso, ipsCA podrá iniciar de oficio el procedimiento de revocación de Certificados,

en cualquiera de los casos previstos en el apartado anterior.

La Autoridad judicial o administrativa podrá, en aquellos supuestos que marque la Ley 59/2003 de 19 de diciembre de firma electrónica así como las demás disposiciones vigentes, instar a ipsCA a revocar el certificado.

La solicitud de revocación de Certificados se podrá dirigir a ipsCA o ante la AR, en su caso, en la forma de BuroFAX o bien personándose físicamente ante la AR, en su caso.

Aquel que solicite la revocación deberá identificarse con cualquier medio válido en derecho y justificar la solicitud aportando la documentación que acredite la existencia del hecho que origina la petición de la revocación.

Cuando la persona que solicite la revocación del certificado TIPO B3 no sea el propio suscriptor, deberá dirigirse en persona a cualquiera de las oficinas de ipsCA o las AR, en su caso.

Una vez recibida y autenticada la solicitud de revocación, ipsCA procederá a tramitar la revocación efectiva del Certificado. La decisión de revocar un Certificado corresponde a ipsCA.

La decisión de revocar el Certificado será comunicada por ipsCA al Suscriptor mediante correo ordinario.

Igualmente, se publicará la revocación del Certificado en la CRL. La publicación de la CRL del ipsCA se realiza cada 24 horas o cada vez que se revoca un certificado. Su consulta se puede realizar vía web en:

<http://www.ipsca.com/crl/ipscab3crl2005.crl>

La revocación comenzará a producir efectos frente a terceros a partir de su publicación por parte de ipsCA, salvo que la causa de revocación sea el cese de la actividad de prestación de servicios de certificación de ipsCA, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

La información relativa al estado de la revocación estará disponible las 24 del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control ipsCA, ipsCA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

#### 6.4.- Renovación del Certificado:

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el suscriptor simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, la CA emitirá una nueva tarjeta y se generarán nuevas claves; pero, únicamente se van a llevar a cabo unas medidas mínimas de comprobación, puesto que el antiguo certificado tiene plena vigencia y nada hacer pensar, salvo que el suscriptor lo exprese, que alguno de sus datos ha cambiado o que ya no es posible confiar en el certificado.

Los certificados emitidos por IPSCA tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación si concurren las circunstancias recogidas en las PC de cada tipo de Certificados.

Los requisitos previos, la forma de solicitar la renovación y el procedimiento de renovación de certificados serán los que se especifiquen en las PC de cada Certificado.

##### **6.4.1 Requisitos previos**

Deberán concurrir los siguientes:

- Que el suscriptor desee la renovación del servicio de certificación antes de que transcurra el año de vigencia de su certificado (con una antelación mínima de 30 días).
- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que IPSCA especifica a tal efecto.
- Que la CA no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación/suspensión del certificado.
- Que no hayan pasado más de cuatro años desde la emisión del primer certificado. Si hubieran pasado más de cuatro años, es decir, la emisión de un certificado y tres renovaciones consecutivas posteriores, el suscriptor deberá someterse a los trámites correspondientes para la emisión de un certificado como cualquier otro solicitante que solicita su certificado por primera vez.

- Que la solicitud de renovación de servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

#### **6.4.2 Cómo solicitar la renovación**

El suscriptor que solicite la renovación de los servicios de certificación deberá cumplimentar un formulario que se encontrará a su disposición en la dirección de Internet de la CA.

El suscriptor enviará ese formulario debidamente cumplimentado a la CA con un plazo de antelación mínimo de 30 días antes de la fecha de caducidad del certificado. El suscriptor deberá manifestar en dicho formulario, bajo su responsabilidad, que ninguno de los datos y circunstancias que constan en su certificado ha variado de alguna forma. Si manifiesta que alguno de estos datos ha cambiado, no procederá la tramitación de este procedimiento.

Además del envío de la solicitud, el suscriptor deberá abonar on-line el precio correspondiente a los servicios que solicita. Esta cantidad se entrega en concepto de tasas de registro, de manera que si el suscriptor no solicitara en debida forma la renovación de su certificado según se establece en la CPS, Prácticas de Certificación aplicables y este mismo manual, no le serán devueltas y no tendrá derecho a reclamarlas a IPSCA.

#### **6.4.3 Procedimiento de renovación de certificados**

Cuando la CA reciba la solicitud del suscriptor en debida forma, procederá a la generación de nuevas claves criptográficas y emitirá una tarjeta inteligente conteniendo el Certificado renovado y que tendrá como fecha de entrada en vigor la del día siguiente a la fecha de caducidad del antiguo certificado.

La CA remitirá esta tarjeta a la correspondiente AR, la cual deberá comunicar en cuanto le sea posible al suscriptor la posibilidad de ir a recogerla, debiendo dirigirse el suscriptor que solicita la renovación a las dependencias de esa AR para recoger la tarjeta y firmar la aceptación del certificado si está conforme.

Con la renovación de los servicios de certificación se entenderá que se mantienen los derechos, obligaciones y responsabilidades tanto de suscriptor como de CA y AR, según se establece en los correspondientes contratos, la CPS y las Prácticas de Certificación aplicables.

Cuando hayan transcurrido más de cuatro años desde la emisión del primer certificado, el Suscriptor no podrá acudir a este método para la renovación de su Certificado y deberá someterse a los trámites correspondientes para la emisión de un nuevo certificado.

#### **6.5.- Validez del Certificado:**

El período de validez máximo del Certificado Tipo B3 es de 4 años, desde su emisión, pasado el cual pierde su vigencia.

Un Certificado que ha perdido su vigencia tiene los mismos efectos de la revocación de un Certificado (6.3.2).

#### **6.6. Aceptación de certificados**

La entrega del certificado y la firma del contrato de adhesión al sistema de certificación implicarán la aceptación del certificado por parte del Firmante.

La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el encargado de ipsCA o de la AR. El solicitante emitirá esta aceptación en su propio nombre y, en su caso, en nombre y representación de la entidad que vaya a ser vinculada por el propio certificado.

No obstante, a partir de la entrega del certificado, el Firmante dispondrá de un periodo de siete días naturales para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a ipsCA y el contenido del certificado, ello deberá ser comunicado de inmediato a ipsCA para que proceda a su revocación y a la emisión de un nuevo certificado. ipsCA entregará el nuevo certificado sin coste para el Firmante en el caso de que la diferencia entre los datos sea causada por un error no imputable al Firmante. Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el Firmante ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, el Firmante confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AR, ipsCA o cualquier tercero que de buena fe confíe en el contenido del Certificado.



---

18 de Mayo de 2005

**Políticas de Certificación (PC)  
Certificados Tipo B3 Colegial**

---

**Anexo II**

**POLÍTICAS DE CERTIFICACIÓN  
De ipsCA**

**Certificados Tipo B3 Colegial**

---

**IPS Certification Authority, s.l.**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52  
Fax 91 640 20 41  
general@ipsca.com  
<http://www.ipsca.com>

## **POLÍTICAS DE CERTIFICACIÓN**

**PC**

**Certificados Tipo B3 Colegial**

Versión 1.0

Fecha de Publicación: Mayo de 2005

PC de ipsCA

Todos los derechos reservados.

EL PRESENTE DOCUMENTO NO PUEDE SER REPRODUCIDO, DISTRIBUIDO, COMUNICADO PÚBLICAMENTE, ARCHIVADO O INTRODUCIDO EN UN SISTEMA DE RECUPERACIÓN DE INFORMACIÓN, O TRANSMITIDO, EN CUALQUIER FORMA Y POR CUALQUIER MEDIO (ELECTRÓNICO, MECÁNICO, FOTOGRÁFICO, GRABACIÓN O CUALQUIER OTRO), TOTAL O PARCIALMENTE, SIN EL PREVIO CONSENTIMIENTO POR ESCRITO DE ipsCA.

### **IPS Certification Authority, s.l.**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52  
Fax 91 640 20 41  
general@ipsca.com  
<http://www.ipsca.com>

**1.- ÍNDICE:**

<b>2.- DEFINICIONES:</b> .....	<b>3</b>
<b>3.- INTRODUCCIÓN</b> .....	<b>5</b>
<b>3.1.- Presentación</b> .....	<b>5</b>
<b>3.2. Estructura</b> .....	<b>5</b>
<b>3.3 Identificación</b> .....	<b>6</b>
<b>3.4 .- Detalles de contacto</b> .....	<b>6</b>
<b>4.- COMUNIDAD DE USUARIOS Y APLICABILIDAD</b> .....	<b>7</b>
<b>4.1.- Prestador de Servicios de Certificación</b> .....	<b>7</b>
<b>4.2.- Autoridad de Registro</b> .....	<b>7</b>
<b>4.3.- Solicitante</b> .....	<b>7</b>
<b>4.4.- Suscriptor</b> .....	<b>7</b>
<b>4.5.- Usuario</b> .....	<b>7</b>
<b>5.- CERTIFICADOS EMITIDOS POR ipsCA</b> .....	<b>8</b>
<b>5.1.- Certificados TIPO B3 Colegial</b> .....	<b>8</b>
<b>6.- CERTIFICADOS TIPO B3 Colegial</b> .....	<b>9</b>
<b>6.1.- Aspectos Generales:</b> .....	<b>9</b>
<b>6.1.1.- Ámbito de aplicación:</b> .....	<b>9</b>
<b>6.1.2.- Datos incluidos en el Certificado:</b> .....	<b>9</b>
<b>6.1.3.- Usos del Certificado y sus límites:</b> .....	<b>11</b>
<b>6.1.4.- Generación de las Claves y del Certificado:</b> .....	<b>13</b>
<b>6.2.- Solicitud del Certificado:</b> .....	<b>13</b>
<b>6.2.1.- Requisitos del Solicitante:</b> .....	<b>13</b>
<b>6.2.2.- Procedimiento de Solicitud, identificación y autenticación y emisión:</b> ..	<b>14</b>
<b>6.3.- Revocación del Certificado:</b> .....	<b>16</b>
<b>6.3.1.- Supuestos de revocación:</b> .....	<b>16</b>
<b>6.3.2.- Efectos de la revocación</b> .....	<b>17</b>
<b>6.3.3.- Procedimiento de revocación:</b> .....	<b>17</b>
<b>6.4.- Renovación del Certificado:</b> .....	<b>19</b>
<b>6.5.- Validez del Certificado:</b> .....	<b>19</b>

## 2.- DEFINICIONES:

- **Acuerdo de Autoridad de Registro:** Contrato suscrito entre ipsCA y una determinada persona física o jurídica, que tiene como objeto regular la relación jurídica entre ambos para una correcta comprobación de identidades para la emisión de Certificados Digitales por parte de ipsCA
- **Autoridad de Registro (AR):** Persona física o jurídica encargada de la comprobación de identidades para la emisión de Certificados Digitales por parte de ipsCA
- **Autoridad de Registro (AR) delegada:** Autoridad de Registro (AR)
- **Certificado (Certificado Digital):** Documento electrónico firmado digitalmente por ipsCA que vincula una clave pública con una determinada persona (física o jurídica) y que tiene como principal finalidad confirmar la identidad de la mencionada persona.
- **Clave Privada:** Clave criptográfica única que el suscriptor utiliza para crear una firma electrónica.
- **Clave Pública:** Clave criptográfica única vinculada a la clave privada que es utilizada para verificar la firma electrónica creada por la clave privada.
- **Contrato de Prestación de Servicios de Certificación:** Contrato que tiene por objeto regular los derechos y obligaciones derivados de la prestación por ipsCA, al suscriptor, de los servicios de Certificación, y, en su caso, la revocación y renovación, del mencionado servicio de Certificación.
- **CRL:** Certificado que tiene por objeto recoger los certificados emitidos y, en su caso, revocados por ipsCA
- **Declaración de Prácticas de Certificación (CPS):** Documento actualizado en el que ipsCA especifica los aspectos más relevantes de la gestión del ciclo de vida de los certificados, incluyendo, aunque no limitado, las condiciones para la solicitud, emisión, uso y revocación de los certificados de ipsCA

- **Documento de identidad válido:** Documento Nacional de Identidad, Pasaporte y demás documentos que la legislación española admita como válidos para acreditar la identidad de una persona.
- **Fedatario Público:** Persona encargada de emitir documentos públicos de acuerdo con las solemnidades requeridas por la legislación española.
- **Firma Electrónica:** Conjunto de datos electrónicos asociados a otros datos electrónicos y vinculados únicamente al suscriptor de un certificado, permitiendo su identificación y que ha sido creada por medios que éste puede tener bajo su exclusivo control y está vinculada a los datos a los que se refiere, lo que permite detectar cualquier modificación posterior de éstos.
- **Políticas de Certificación (PC):** Documento actualizado en el que ipsCA especifica un conjunto de reglas que señalan los procedimientos seguidos por ipsCA en relación a la solicitud, identificación y revocación de un certificado, así como los límites de uso, el ámbito de aplicación y las características técnicas de cada tipo de certificado.
- **Prestador de Servicios de Certificación:** Persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica.
- **Solicitante:** Persona física o jurídica, que actúa en nombre propio o en el de una persona jurídica a la que representa, y que está autorizada, en función de cada una de las PC de cada Certificado, a solicitar un Certificado Digital.
- **Suscriptor:** Persona física o jurídica a favor de la cual se ha emitido un Certificado Digital y que posee un Certificado y lo utiliza de acuerdo con las Políticas de Certificación.
- **Usuario:** Persona que voluntariamente confía y hace uso de los Certificados de ipsCA

### **3.- INTRODUCCIÓN**

#### **3.1.- Presentación**

El presente documento recoge la Política de Certificación (PC) de ipsCA para los Certificados Personales Tipo B3. Esta PC pormenoriza y completa lo establecido en la CPS de ipsCA, recogiendo un conjunto de reglas que indican los procedimientos seguidos por ipsCA en la prestación de sus servicios (solicitud, identificación, aceptación y revocación) así como los límites de uso, el ámbito de aplicación y las características técnicas de este tipo de certificado.

Esta Política de Certificación (PC), junto con la CPS de ipsCA, están dirigidas a cualquiera que confíe de buena fe en este tipo de certificados.

#### **3.2. Estructura**

La estructura de esta PC es la siguiente:

- 1 ÍNDICE**
- 2 DEFINICIONES**
- 3 INTRODUCCIÓN**
  - 3.1 Presentación**
  - 3.2 Estructura**
  - 3.3 Identificación**
  - 3.4 Detalles de contacto**
- 4 COMUNIDAD DE USUARIOS Y APLICABILIDAD**
  - 4.1 Prestador de Servicios de certificación**
  - 4.2 Autoridad de Registro**
  - 4.3 Solicitante**
  - 4.4 Suscriptor**
  - 4.5 Usuario**
- 5 CERTIFICADOS EMITIDOS POR ipsCA**
  - 5.1 Certificados Tipo B3 Colegial**
- 6 CERTIFICADOS TIPO B3 Colegial**
  - 6.1 Aspectos Generales**
    - 6.1.1 Ámbito de Aplicación**

- 6.1.2 Datos incluidos en el Certificado**
- 6.1.3 Usos del Certificado y sus límites**
- 6.1.4 Generación de las Claves y del Certificado**
- 6.2 Solicitud del Certificado**
  - 6.2.1 Requisitos del Solicitante**
  - 6.2.2 Procedimiento de Solicitud, identificación y autenticación y emisión**
- 6.3 Revocación del Certificado**
  - 6.3.1 Supuestos de revocación**
  - 6.3.2 Efectos de la revocación**
  - 6.3.3 Procedimiento de revocación**
- 6.4 Renovación del Certificado**
  - 6.4.1. Requisitos previos**
  - 6.4.2. Cómo solicitar la renovación**
  - 6.4.3 Procedimiento de renovación**
- 6.5 Validez del Certificado**
- 6.6 Aceptación de Certificados**

### **3.3 Identificación**

Esta PC puede ser consultada por Internet en el servidor web de ipsCA, <http://www.ipsca.com> o personalmente en las oficinas de ipsCA.

Todos los solicitantes y suscriptores de certificados manifiestan que conocen este documento, antes de la petición de cualquier tipo de certificado a ipsCA y además conocen el funcionamiento de los sistemas de clave pública en que se basan los certificados digitales.

### **3.4 .- Detalles de contacto**

#### **IPS Certification Authority, s.l.**

Edificio ECU  
Ctra. de La Coruña, Km. 23,200  
28290 - Parque Rozas  
(Madrid)  
Tel. 91 640 20 52

## **4.- COMUNIDAD DE USUARIOS Y APLICABILIDAD**

### **4.1.- Prestador de Servicios de Certificación**

ipsCA actúa como Autoridad Certificadora (CA) relacionando una determinada clave pública con un sujeto, entidad o sitio Web concretos a través de la emisión de un Certificado de conformidad con los términos de estas PC y con el CPS de ipsCA.

### **4.2.- Autoridad de Registro**

ipsCA delega la comprobación de identidades en una o varias Autoridades de Registro (AR). Esta delegación se formalizará en un Acuerdo para Autoridad de Registro. Las autoridades de registro delegadas deberán comprobar la identidad de los solicitantes de acuerdo con las normas de estas PC, de la CPS y del Acuerdo para Autoridad de Registro.

### **4.3.- Solicitante**

A los efectos de estas PC, se entenderá por Solicitante a la persona física o jurídica, que actúa en nombre propio o en el de una persona jurídica a la que representa, y que está autorizada, en función de cada una de las PC de cada Certificado, que se detallan más adelante, a solicitar un Certificado Digital..

### **4.4.- Suscriptor**

El suscriptor será la persona física o jurídica a favor de la cual se ha emitido un Certificado Digital.

Los suscriptores deberán ajustarse a lo señalado en las PC, en la CPS y, en su caso, en contrato de Prestación de Servicios suscrito con ipsCA.

### **4.5.- Usuario**

Se entiende por Usuario del Certificado a la persona que voluntariamente confía y hace uso de los Certificados de ipsCA.

Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación las presentes PC, así como la CPS.

## **5.- CERTIFICADOS EMITIDOS POR ipsCA:**

### **5.1.- B1. Certificado de Correo con validez mensual/anual.**

En él se relaciona el nombre que introduzca en nuestro cuestionario con una cuenta de correo válida. Permite la firma y encriptación de correo.

No tiene carácter comercial pues no existe comprobación de la identidad del sujeto.

Toda la información contenida en el certificado es suministrada por la entidad que actúa como Autoridad de Registro bajo su entera responsabilidad, o por el propio usuario y resulta como información del suscriptor no verificada, de acuerdo con lo establecido en el presente CPS.

### **5.2. B3. Certificado Personal Presencial.**

ipsCA emite Certificados que permiten la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en esta CPS, en la PC de los Certificados Personales B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

La comprobación de la persona será presencial y documental. El individuo deberá presentarse ante la AR con un documento de identidad válido. LA AR puede ser un departamento de una empresa o cualquier otro tipo de Autoridad de Registro debidamente homologada por la CA

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la práctica oficial aplicable en función de la concreta Autoridad de Registro, y que debe consultarse en las Prácticas Certificación correspondientes.

### **5.3. B3. Colegial**

ipsCA emite Certificados que permiten la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor, su pertenencia a un Colegio profesional y con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en esta CPS, en la PC de los Certificados Personales B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

La comprobación de la persona será presencial y documental. El individuo deberá presentarse ante la AR con un documento de identidad válido. La AR será el colegio profesional para el que se emiten los certificados

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la práctica oficial aplicable en función de la concreta Autoridad de Registro, y que debe consultarse en las Prácticas Certificación correspondientes.

### **5.4 A1. Certificado de Servidor**

Los Certificados de Servidor de permiten incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta, passwords, etc. Cobra especial importancia dentro del área del comercio electrónico, donde la seguridad de los datos es la principal lacra para el desarrollo de este sistema.

La emisión de un certificado de servidor implica tener registrado el dominio de Internet bajo el que se denomina el servidor y cumplir con el procedimiento que en el punto 3.3.5 se detalla.

ipsCA emite Certificados que posibilitan la realización de la firma electrónica avanzada según lo dispuesto en la Ley 59/2003 de 19 de diciembre de firma electrónica. En este tipo de Certificados se relaciona la identidad de un suscriptor con su clave pública. Permite la firma de documentos electrónicos.

La comprobación de la identidad del solicitante/suscriptor será presencial y documental. El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro con un documento de identidad válido.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en la CPS, en esta PC de los Certificados Tipo B3 y, en su caso, con lo recogido en el Acuerdo para Autoridad de Registro.

## **6.- CERTIFICADOS TIPO B3 Colegial**

### **6.1.- Aspectos Generales:**

#### 6.1.1.- Ámbito de aplicación:

En este tipo de Certificados se relaciona la identidad de un suscriptor y su pertenencia a un colegio profesional con su clave pública, permite la firma de documentos electrónicos.

Por ello les será de aplicación las normas españolas referidas a la firma electrónica y, especialmente, la Ley 59/2003 de 19 de diciembre de firma electrónica

#### 6.1.2.- Datos incluidos en el Certificado:

Los datos que se incluirán en un Certificado Clase 3 Reconocido emitido por ipsCA serán los siguientes:

#### **Asunto:**

CN= "NOMBRE" blanco *NOMBRE* blanco 1<sup>er</sup> *APELLIDO* blanco 2º *APELLIDO* blanco "–  
" blanco "NIF" blanco *NIF CON 9 DIGITOS* blanco "–" *NC con 8 dígitos*

OU= *Departamento*

O= *Colegio Profesional*

L= Localidad donde se encuentre empadronado el suscriptor

S= Provincia donde se encuentre empadronado el suscriptor

C="ES"

E= Dirección de correo electrónico del suscriptor

#### **Extensiones estándar**

#### **Extensiones especiales**

Se incluye el parseo de un Certificado Tipo B3 de Colegial de prueba:

0:d=0 hl=4 l=1417 cons: SEQUENCE  
 4:d=1 hl=4 l=1137 cons: SEQUENCE  
 8:d=2 hl=2 l= 3 cons: cont [ 0 ]  
 10:d=3 hl=2 l= 1 prim: INTEGER :02  
 13:d=2 hl=2 l= 10 prim: INTEGER :1285EA01000000000152  
 25:d=2 hl=2 l= 13 cons: SEQUENCE  
 27:d=3 hl=2 l= 9 prim: OBJECT :sha1WithRSAEncryption  
 38:d=3 hl=2 l= 0 prim: NULL  
 40:d=2 hl=3 l= 183 cons: SEQUENCE  
 43:d=3 hl=2 l= 11 cons: SET  
 45:d=4 hl=2 l= 9 cons: SEQUENCE  
 47:d=5 hl=2 l= 3 prim: OBJECT :countryName  
 52:d=5 hl=2 l= 2 prim: PRINTABLESTRING :ES  
 56:d=3 hl=2 l= 18 cons: SET  
 58:d=4 hl=2 l= 16 cons: SEQUENCE  
 60:d=5 hl=2 l= 3 prim: OBJECT :stateOrProvinceName  
 65:d=5 hl=2 l= 9 prim: PRINTABLESTRING :Barcelona  
 76:d=3 hl=2 l= 18 cons: SET  
 78:d=4 hl=2 l= 16 cons: SEQUENCE  
 80:d=5 hl=2 l= 3 prim: OBJECT :localityName  
 85:d=5 hl=2 l= 9 prim: PRINTABLESTRING :Barcelona  
 96:d=3 hl=2 l= 25 cons: SET  
 98:d=4 hl=2 l= 23 cons: SEQUENCE  
 100:d=5 hl=2 l= 3 prim: OBJECT :organizationName  
 105:d=5 hl=2 l= 16 prim: PRINTABLESTRING :IPS Seguridad CA  
 123:d=3 hl=2 l= 24 cons: SET  
 125:d=4 hl=2 l= 22 cons: SEQUENCE  
 127:d=5 hl=2 l= 3 prim: OBJECT :organizationalUnitName  
 132:d=5 hl=2 l= 15 prim: PRINTABLESTRING :Certificaciones  
 149:d=3 hl=2 l= 43 cons: SET  
 151:d=4 hl=2 l= 41 cons: SEQUENCE  
 153:d=5 hl=2 l= 3 prim: OBJECT :commonName  
 158:d=5 hl=2 l= 34 prim: PRINTABLESTRING :CLASE B-3 ipsCA-IPS Seguridad  
 2005  
 194:d=3 hl=2 l= 30 cons: SET  
 196:d=4 hl=2 l= 28 cons: SEQUENCE  
 198:d=5 hl=2 l= 9 prim: OBJECT :emailAddress

209:d=5 hl=2 l= 15 prim: IA5STRING :ips@mail.ips.es  
 226:d=2 hl=2 l= 30 cons: SEQUENCE  
 228:d=3 hl=2 l= 13 prim: UTCTIME :050525114712Z  
 243:d=3 hl=2 l= 13 prim: UTCTIME :070525115712Z  
 258:d=2 hl=3 l= 192 cons: SEQUENCE  
 261:d=3 hl=2 l= 36 cons: SET  
 263:d=4 hl=2 l= 34 cons: SEQUENCE  
 265:d=5 hl=2 l= 9 prim: OBJECT :emailAddress  
 276:d=5 hl=2 l= 21 prim: IA5STRING :DIRECCION @CORREO.COM  
 299:d=3 hl=2 l= 11 cons: SET  
 301:d=4 hl=2 l= 9 cons: SEQUENCE  
 303:d=5 hl=2 l= 3 prim: OBJECT :countryName  
 308:d=5 hl=2 l= 2 prim: PRINTABLESTRING :ES  
 312:d=3 hl=2 l= 18 cons: SET  
 314:d=4 hl=2 l= 16 cons: SEQUENCE  
 316:d=5 hl=2 l= 3 prim: OBJECT :stateOrProvinceName  
 321:d=5 hl=2 l= 9 prim: PRINTABLESTRING :PROVINCIA  
 332:d=3 hl=2 l= 15 cons: SET  
 334:d=4 hl=2 l= 13 cons: SEQUENCE  
 336:d=5 hl=2 l= 3 prim: OBJECT :localityName  
 341:d=5 hl=2 l= 6 prim: PRINTABLESTRING :CIUDAD  
 349:d=3 hl=2 l= 16 cons: SET  
 351:d=4 hl=2 l= 14 cons: SEQUENCE  
 353:d=5 hl=2 l= 3 prim: OBJECT :organizationName  
 358:d=5 hl=2 l= 7 prim: PRINTABLESTRING :EMPRESA  
 367:d=3 hl=2 l= 21 cons: SET  
 369:d=4 hl=2 l= 19 cons: SEQUENCE  
 371:d=5 hl=2 l= 3 prim: OBJECT :organizationalUnitName  
 376:d=5 hl=2 l= 12 prim: PRINTABLESTRING :DEPARTAMENTO  
 390:d=3 hl=2 l= 61 cons: SET  
 392:d=4 hl=2 l= 59 cons: SEQUENCE  
 394:d=5 hl=2 l= 3 prim: OBJECT :commonName  
 399:d=5 hl=2 l= 52 prim: PRINTABLESTRING :NOMBRE RECONOCIDO PRUEBA  
 CERTIFICADO - NIF 00000000Z  
 453:d=2 hl=3 l= 159 cons: SEQUENCE  
 456:d=3 hl=2 l= 13 cons: SEQUENCE  
 458:d=4 hl=2 l= 9 prim: OBJECT :rsaEncryption

469:d=4 hl=2 l= 0 prim: NULL  
 471:d=3 hl=3 l= 141 prim: BIT STRING  
 615:d=2 hl=4 l= 526 cons: cont [ 3 ]  
 619:d=3 hl=4 l= 522 cons: SEQUENCE  
 623:d=4 hl=2 l= 14 cons: SEQUENCE  
 625:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Key Usage  
 630:d=5 hl=2 l= 1 prim: BOOLEAN :255  
 633:d=5 hl=2 l= 4 prim: OCTET STRING  
 639:d=4 hl=2 l= 29 cons: SEQUENCE  
 641:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Extended Key Usage  
 646:d=5 hl=2 l= 22 prim: OCTET STRING  
 670:d=4 hl=2 l= 29 cons: SEQUENCE  
 672:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Subject Key Identifier  
 677:d=5 hl=2 l= 22 prim: OCTET STRING  
 701:d=4 hl=3 l= 210 cons: SEQUENCE  
 704:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Authority Key Identifier  
 709:d=5 hl=3 l= 202 prim: OCTET STRING  
 914:d=4 hl=2 l= 108 cons: SEQUENCE  
 916:d=5 hl=2 l= 3 prim: OBJECT :X509v3 CRL Distribution Points  
 921:d=5 hl=2 l= 101 prim: OCTET STRING  
 1024:d=4 hl=2 l= 119 cons: SEQUENCE  
 1026:d=5 hl=2 l= 8 prim: OBJECT :Authority Information Access  
 1036:d=5 hl=2 l= 107 prim: OCTET STRING  
 1145:d=1 hl=2 l= 13 cons: SEQUENCE  
 1147:d=2 hl=2 l= 9 prim: OBJECT :sha1WithRSAEncryption  
 1158:d=2 hl=2 l= 0 prim: NULL  
 1160:d=1 hl=4 l= 257 prim: BIT STRING

### 6.1.3.- Usos del Certificado y sus límites:

Este tipo de Certificado se utilizará, principalmente, para firmar electrónicamente, documentos electrónicos Con este hecho se garantiza:

*Identificación del firmante* El Firmante del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.

*Integridad del documento firmado:* La utilización de este Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Firmante. Se certifica que el mensaje recibido por el Tercero que confía es el mismo que fue emitido por el Firmante

*No repudio de origen:* Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Firmante que ha firmado no puede negar la autoría o la integridad del mismo.

Este Certificado se podrá utilizar, para la firma de mensajes de correo electrónico que soporten protocolo S/MIME y para la autenticación en servidores web seguros utilizando el protocolo SSL 3.0

Por las características esenciales del certificado éste podría ser utilizado para otras finalidades y, en concreto, para el cifrado y descifrado de documentos o mensajes electrónicos. No obstante, este uso es de exclusiva responsabilidad del suscriptor y/o el usuario del certificado, ipsCA no asume ningún tipo de responsabilidad, ya sea legal, contractual o extra contractual, derivada de daños directos o indirectos por la utilización del certificado para tal finalidad, debido a que, por motivos de seguridad, esta Política determina que ipsCA no guarde copia de la clave privada del Firmante.

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso.

El empleo de los certificados que implique la realización de operaciones no autorizadas según las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los Contratos de ipsCA con sus Firmantes tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto ipsCA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el Firmante o cualquier tercero.

En función de los servicios prestados por ipsCA mediante la emisión de sus certificados, no es posible por parte de ipsCA el acceso o conocimiento del contenido del mensaje al que haya sido adjuntado o con el que se relacione el uso de un certificado emitido por ipsCA. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de ipsCA emitir valoración alguna sobre dicho contenido, asumiendo por tanto el signatario cualquier responsabilidad dimanante del contenido de

dicho mensaje aparejado al uso de un certificado emitido por ipsCA.

Asimismo, le será imputable al signatario cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificación aplicables a cada uno de los Certificados, la CPS y los contratos de ipsCA con sus Firmantes, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación española vigente sobre firma electrónica

#### 6.1.4.- Generación de las Claves y del Certificado:

El soporte para el almacenamiento de las claves y el certificado será siempre:

Una tarjeta o dispositivo criptográfico. El acceso al dispositivo criptográfico, donde se encuentra la clave privada, se realizará a través de contraseña (PIN). Para realizar una firma electrónica es necesario introducir el PIN que únicamente debe conocer el suscriptor. En la generación de las claves no se permite realizar una copia de seguridad de las mismas.

#### 6.2.- Solicitud del Certificado:

##### 6.2.1.- Requisitos del Solicitante:

Para ser solicitante y, en su caso y posteriormente, ser suscriptor de este tipo de certificados, es necesario cumplir con estos requisitos:

Ser persona física

Poseer un Documento de identidad válido.

Pertenecer a un Colegio Profesional

##### 6.2.2.- Procedimiento de Solicitud, identificación y autenticación y emisión:

El usuario se presentará ante la AR y acreditará su identidad mostrando a la AR un Documento de Identidad válido.

Todos los Firmantes requieren un nombre distintivo (DN o distinguished name)

conforme al estándar X.500. Los pseudónimos no serán admitidos.

Tras autenticar al usuario y comprobar los datos el ipsCA emitirá el certificado y se lo entregará de manera segura al usuario.

## Emisión

1. El operador de la CA introduce en el lector de tarjetas o el dispositivo criptográfico, que está conectado al módulo de emisión y validación de certificados, la tarjeta o dispositivo preimpresa del solicitante.

2. El módulo de validación y emisión de Certificados ejecuta las siguientes operaciones:  
Genera automáticamente las claves (pública y privada) en la propia tarjeta o dispositivo criptográfico.

Envía el CSR (Petición de certificado) a la CA donde se firmará en modo automático.

El certificado es devuelto por la CA e instalado en la tarjeta o dispositivo.

3. La tarjeta o dispositivo criptográfico dispone de un PIN de acceso conocido por defecto cuando aún no contiene un certificado. El módulo de validación y emisión de Certificados introduce el PIN por defecto de manera automática, para acceder a la tarjeta. Tras instalar el certificado emitido, genera un PIN aleatorio basado en una combinación de 10 dígitos alfanuméricos que introduce en la tarjeta criptográfica.

Nota: En ningún momento del proceso, el operador de la CA tiene acceso al PIN aleatorio generado por el módulo de emisión. De esta manera, se garantiza que la firma electrónica generada cumple los requisitos para ser considerada firma electrónica avanzada según el artículo 3.2 de la LFE al ser solo el suscriptor de la firma el que conoce el PIN de acceso a la tarjeta criptográfica.

4. La aplicación genera automáticamente una carta en papel autocopiativo inverso conteniendo el PIN impreso para su envío por correo postal al suscriptor de la firma. Además se imprimen tres copias del "Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA, personalizado con los datos del Certificado y del solicitante.

5. Se remite al domicilio del solicitante el PIN definitivo

6. La Tarjeta que contiene el Certificado, junto con las tres copias del documento antes mencionado se remiten a la AR.

## Entrega

Una vez que el usuario ha recibido la carta con el PIN, debe acudir personalmente a la AR en un plazo de 30 días. Queda totalmente prohibida la asistencia en nombre o representación de otra persona.

El solicitante debe aportar a la AR su DNI y su Tarjeta de Colegiado para demostrar su identidad.

Si el solicitante no acude en el mencionado plazo a la AR, se procede a la revocación del certificado y la devolución ipsCA del soporte que lo contenga donde se destruye físicamente

El operador de la AR comprueba que los datos incluidos en el DNI y en la Tarjeta de colegiado coinciden con los datos impresos en la tarjeta criptográfica y que coinciden, además, con los del “Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA

El solicitante debe comprobar en la propia AR que los datos del certificado son correctos y se corresponden con los suyos.

El agente autorizado para la verificación de identidad de la AR y el solicitante deben firmar las tres copias del documento “Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA

Además el agente autorizado para la verificación de identidad de la AR entrega, en su caso, el Kit compuesto por el lector de tarjetas, un CD con software necesario para la firma de archivos PDF y el manual de instrucciones.

El agente autorizado para la verificación de identidad de la AR archiva una copia firmada del “Documento de certificación de identidad y de información, conocimiento y aceptación del certificado Tipo B3 de ipsCA”, entregará al solicitante otra de las copias firmadas y la

tercera será remitida en un plazo no superior a siete días al ipsCA

### **6.3.- Revocación del Certificado:**

#### **6.3.1.- Supuestos de revocación:**

Los Certificados Clase 3 deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

1.

- Solicitud voluntaria del Suscriptor.
- Pérdida o inutilización por daños del soporte del certificado o modificación del certificado.
- Utilización indebida del certificado por el suscriptor o por terceros.
- Fallecimiento del suscriptor.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Por error en la emisión del certificado debido a una no adecuación al procedimiento establecido en las PC establecidas para los Certificados Tipo B3 y/o, en su caso, en el contrato establecido entre ipsCA y el suscriptor.
- Que se detecte que las claves privadas del Suscriptor o de ipsCA han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la AR, ipsCA o el Suscriptor de las obligaciones establecidas en la CPS.
- Por la resolución del contrato.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la CPS o en las presentes PC establecidas para cada tipo de Certificado.

En cualquier caso, todas las solicitudes deberán ser autenticadas.

### 6.3.2.- Efectos de la revocación

El efecto de la revocación del Certificado Clase 3 es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La revocación del Certificado por causa no imputable al Suscriptor originará la emisión de un nuevo Certificado a favor del Suscriptor por el plazo equivalente al restante para concluir el período originario de validez del Certificado revocado.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.

### 6.3.3.- Procedimiento de revocación:

Deberán solicitar la revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- El Suscriptor del Certificado TIPO B3 Colegial
- La AR, respecto a aquellos Certificados en cuya emisión hayan participado.
- El Colegio Profesional al que pertenece el suscriptor.

Asimismo, podrá solicitar la revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del Certificado.
- Fallecimiento del suscriptor.
- Incapacidad sobrevenida, total o parcial.
- Inexactitudes en el certificado.
- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.

En todo caso, ipsCA podrá iniciar de oficio el procedimiento de revocación de Certificados, en cualquiera de los casos previstos en el apartado anterior.

La Autoridad judicial o administrativa podrá, en aquellos supuestos que marque la Ley 59/2003 de 19 de diciembre de firma electrónica así como las demás disposiciones vigentes, instar a ipsCA a revocar el certificado.

La solicitud de revocación de Certificados se podrá dirigir a ipsCA o ante la AR, en su caso, en la forma de BuroFAX o bien personándose físicamente ante la AR, en su caso.

Aquel que solicite la revocación deberá identificarse con cualquier medio válido en derecho y justificar la solicitud aportando la documentación que acredite la existencia del hecho que origina la petición de la revocación.

Cuando la persona que solicite la revocación del certificado TIPO B3 no sea el propio suscriptor, deberá dirigirse en persona a cualquiera de las oficinas de ipsCA o las AR, en su caso.

Una vez recibida y autenticada la solicitud de revocación, ipsCA procederá a tramitar la revocación efectiva del Certificado. La decisión de revocar un Certificado corresponde a ipsCA.

La decisión de revocar el Certificado será comunicada por ipsCA al Suscriptor mediante correo ordinario.

Igualmente, se publicará la revocación del Certificado en la CRL. La publicación de la CRL de ipsCA se realiza cada 24 horas o cada vez que se revoca un certificado. Su consulta se puede realizar vía web en:

<http://www.ipsca.com/crl/ipscab3crl2005.crl>

La revocación comenzará a producir efectos frente a terceros a partir de su publicación por parte de ipsCA, salvo que la causa de revocación sea el cese de la actividad de prestación de servicios de certificación de ipsCA, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

La información relativa al estado de la revocación estará disponible las 24 del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control ipsCA, ipsCA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

#### **6.4.- Renovación del Certificado:**

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el suscriptor simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, la CA emitirá una nueva tarjeta y se generarán nuevas claves; pero, únicamente se van a llevar a cabo unas medidas mínimas de comprobación, puesto que el antiguo certificado tiene plena vigencia y nada hacer pensar, salvo que el suscriptor lo exprese, que alguno de sus datos ha cambiado o que ya no es posible confiar en el certificado.

Los certificados emitidos por IPSCA tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación si concurren las circunstancias recogidas en las PC de cada tipo de Certificados.

Los requisitos previos, la forma de solicitar la renovación y el procedimiento de renovación de certificados serán los que se especifiquen en las PC de cada Certificado.

##### **6.4.1 Requisitos previos**

Deberán concurrir los siguientes:

- Que el suscriptor desee la renovación del servicio de certificación antes de que transcurra el año de vigencia de su certificado (con una antelación mínima de 30 días).

- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que IPSCA especifica a tal efecto.
- Que la CA no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación/suspensión del certificado.
- Que no hayan pasado más de cuatro años desde la emisión del primer certificado. Si hubieran pasado más de cuatro años, es decir, la emisión de un certificado y tres renovaciones consecutivas posteriores, el suscriptor deberá someterse a los trámites correspondientes para la emisión de un certificado como cualquier otro solicitante que solicita su certificado por primera vez.
- Que la solicitud de renovación de servicios de prestación se refiera al mismo tipo de certificado emitido inicialmente.

#### **6.4.2 Cómo solicitar la renovación**

El suscriptor que solicite la renovación de los servicios de certificación deberá cumplimentar un formulario que se encontrará a su disposición en la dirección de Internet de la CA.

El suscriptor enviará ese formulario debidamente cumplimentado a la CA con un plazo de antelación mínimo de 30 días antes de la fecha de caducidad del certificado. El suscriptor deberá manifestar en dicho formulario, bajo su responsabilidad, que ninguno de los datos y circunstancias que constan en su certificado ha variado de alguna forma. Si manifiesta que alguno de estos datos ha cambiado, no procederá la tramitación de este procedimiento.

Además del envío de la solicitud, el suscriptor deberá abonar on-line el precio correspondiente a los servicios que solicita. Esta cantidad se entrega en concepto de tasas de registro, de manera que si el suscriptor no solicitara en debida forma la renovación de su certificado según se establece en la CPS, Prácticas de Certificación aplicables y este mismo manual, no le serán devueltas y no tendrá derecho a reclamarlas a IPSCA.

#### **6.4.3 Procedimiento de renovación de certificados**

Cuando la CA reciba la solicitud del suscriptor en debida forma, procederá a la generación de nuevas claves criptográficas y emitirá una tarjeta inteligente conteniendo el Certificado renovado y que tendrá como fecha de entrada en vigor la del día siguiente a la fecha de caducidad del antiguo certificado.

La CA remitirá esta tarjeta a la correspondiente AR, la cual deberá comunicar en cuanto le sea posible al suscriptor la posibilidad de ir a recogerla, debiendo dirigirse el suscriptor que solicita la renovación a las dependencias de esa AR para recoger la tarjeta y firmar la aceptación del certificado si está conforme.

Con la renovación de los servicios de certificación se entenderá que se mantienen los derechos, obligaciones y responsabilidades tanto de suscriptor como de CA y AR, según se establece en los correspondientes contratos, la CPS y las Prácticas de Certificación aplicables.

Cuando hayan transcurrido más de cuatro años desde la emisión del primer certificado, el Suscriptor no podrá acudir a este método para la renovación de su Certificado y deberá someterse a los trámites correspondientes para la emisión de un nuevo certificado.

#### **6.5.- Validez del Certificado:**

El período de validez máximo del Certificado Tipo B3 es de 4 años, desde su emisión, pasado el cual pierde su vigencia.

Un Certificado que ha perdido su vigencia tiene los mismos efectos de la revocación de un Certificado (6.3.2).

#### **6.6. Aceptación de certificados**

La entrega del certificado y la firma del contrato de adhesión al sistema de certificación implicará la aceptación del certificado por parte del Firmante.

La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el encargado de ipsCA o de la AR. El solicitante emitirá esta aceptación en su propio nombre y, en su caso, en nombre y representación de la entidad que vaya a ser vinculada por el propio certificado.

No obstante, a partir de la entrega del certificado, el Firmante dispondrá de un periodo de siete días naturales para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a ipsCA y el contenido del certificado, ello deberá ser comunicado de inmediato a ipsCA para que proceda a su revocación y a la emisión de un nuevo certificado. ipsCA entregará el nuevo certificado sin coste para el Firmante en el caso de que la diferencia entre los datos sea causada por un error no imputable al Firmante.

Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el Firmante ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, el Firmante confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AR, ipsCA o cualquier tercero que de buena fe confíe en el contenido del Certificado.